

# Thus Spoke...The Gentlemen

By stcpresearch

Published: 2026-05-13 · Archived: 2026-05-22 02:01:25 UTC

## Key Points

- On May 4th, 2026, **The Gentlemen RaaS** administrator acknowledged on underground forums that an internal backend database (**Rocket**) had been leaked. This leak exposed **9 accounts**, including **zeta88** (aka **hastalamuerte**), who runs the infrastructure, builds the locker and **RaaS** panel, manages payouts, and effectively acts as the administrator of the program.
- The internal discussions provide a rare **end-to-end view** of the operation: they detail initial access paths (Fortinet and Cisco edge appliances, NTLM relay, OWA/M365 credential logs), the division of roles, the shared toolsets, and the group's active tracking and evaluation of modern CVEs such as **CVE-2024-55591**, **CVE-2025-32433**, and **CVE-2025-33073**.
- Screenshots from ransom negotiations were also leaked, showing a successful case where the group received **190,000 USD**, after starting with an initial demand (anchor) of **250,000 USD**.
- Further chats indicate that stolen data from a UK software consultancy was later reused to attack a company in Turkey. The Gentlemen used this during negotiations as a dual-pressure tactic: they portrayed the UK firm as the "access broker," while mentioning to provide "proof" to the Turkish company that the intrusion originated from the UK side and encouraging it to consider legal action against the consultancy.
- By collecting all available ransomware samples, Check Point Research identified **8 distinct affiliate TOX IDs**, including the administrator's TOX ID. This suggests that the admin not only manages the **RaaS** program but also actively participates in, or directly carries out, some of the infections.

## Introduction

The Gentlemen ransomware-as-a-service (**RaaS**) operation is a relatively new group that emerged around mid-2025. Its operators advertise the service across multiple underground forums, promoting their ransomware platform and inviting penetration testers and other technically skilled actors to join as affiliates.

In 2026, based on victims listed on the data leak site (DLS), The Gentlemen appears to be **one of the most active RaaS programs**, with approximately **332 published victims** in just the first five months of 2026. This volume places the group as the **second most productive RaaS operation** in that period, at least among those that publicly list their victims.

During our previous [publication](#), Check Point Research analyzed a specific infection carried out by an affiliate of this RaaS. In that case, the affiliate used `SystemBC`, and the associated command-and-control (C&C) server revealed more than **1,570 victims**.

In this publication, we focus on the affiliate program itself and the actors who participate in it. On May 4th, 2026, The Gentlemen administrator acknowledged the leak of an internal database used by the group, which contained operational information about their infrastructure, affiliates, and victims. Check Point Research obtained what appears to be a partial leak of the group's internal chats and related data, which was briefly posted on an underground forum before being removed. Later on, the leak also appeared on another underground forum.

The leaked material includes detailed conversations between the RaaS operators and their affiliates across several internal channels (such as `INFO`, `general`, `TOOLS`, and `PODBOR`). In these chats, they coordinate ongoing intrusions, exchange toolsets and EDR-kill packages, discuss infrastructure and backend components (including the **Rocket** database and NAS storage), review CVEs and exploit paths (for example Fortinet, Cisco, and NTLM relay issues), and talk about specific victims, campaigns, and payouts. Together, these messages provide a rare inside view of how The Gentlemen plans, executes, and scales its ransomware operations.

## The Gentlemen RaaS Admin

The Gentlemen RaaS administrator has been very active and vocal on various underground forums, trying to attract affiliates with an aggressive profit-sharing model: **90%** for affiliates and **10%** for the operator.

In [September 2025](#), in one of the first posts promoting the RaaS program, the account **Zeta88** published a message advertising the service and inviting individual penetration testers to join as affiliates.



Figure 1 — Zeta88 advertising The Gentlemen's RaaS.

Later on, the official posts for this ransomware program started to be published by another account, **The Gentlemen**. The administrator also shared their TOX ID across several forums.



Figure 2 — RaaS admin in underground forum.

The same TOX ID can be seen on the onion data leak site (DLS), where it is used by affiliates or compromised victims to contact the administrator.



Figure 3 — Onion page TOX ID.

In a post on an underground forum, where the administrator demonstrated how affiliates can build the ransomware, we can see the administrator's profile page, where their TOX ID is again visible in the corresponding field.



Figure 4 — Image uploaded by RaaS admin.

In the second shared image, we again observe the same TOX ID and see how the target or victim entry is supposed to look from an affiliate's perspective.



Figure 5 — Image uploaded by RaaS admin.

Considering that the initial post was made by `Zeta88`, it is likely that this account belongs to the administrator and that their TOX ID is `F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EB8DF92CF9A9B84079F8F04060FF98D098E`. This assessment is based on the fact that the same TOX ID appears consistently across different contexts: in the early recruitment posts, in the onion data leak site (DLS), and in the screenshots showing the administrator's profile and communication fields. Taken together, these overlaps strongly suggest that `Zeta88`, the later `The Gentlemen` account, and this TOX ID are all controlled by the same RaaS administrator.

## RaaS Affiliates

Check Point Research collected most of the available artifacts related to The Gentlemen RaaS from online sources. Based on the current **412 public victims** listed on the data leak site (DLS), and considering that there are likely additional victims who paid and therefore were not published, we identified **29 unique campaigns** in public sources such as VirusTotal.

For each of these 29 campaigns, we extracted the TOX ID associated with the corresponding affiliate. Our analysis shows that these campaigns were conducted by **8 unique TOX IDs**.

Plain text

Copy to clipboard

Open code in new window

EnlighterJS 3 Syntax Highlighter

```
15CE8D5DB0BAC3BCBB1FA69F2E672CC54EFBEC7684DA792F3CBF8B007A9FEA1D16374560DFA5
2F1A9C8B8AA163BBB84FF799A0954B232C279C5E9EE42505955288EAD28685A2BC0713C7745
88984846080D639C9A4EC394E53BA616D550B2B3AD691942EA2CCD33AA5B9340FD1A8FF40E9A
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69
D527959A7BC728CB272A0DB683B547F079C98012201A48DD2792B84604E8BC29F6E6BDB8003F
F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E
F96C481CBB0D6E7BDA49C6D68CFDB1D284354961534EDEEDA854C672B48A8D6B7146F90BDACB

15CE8D5DB0BAC3BCBB1FA69F2E672CC54EFBEC7684DA792F3CBF8B007A9FEA1D16374560DFA5
2F1A9C8B8AA163BBB84FF799A0954B232C279C5E9EE42505955288EAD28685A2BC0713C7745
88984846080D639C9A4EC394E53BA616D550B2B3AD691942EA2CCD33AA5B9340FD1A8FF40E9A
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69
D527959A7BC728CB272A0DB683B547F079C98012201A48DD2792B84604E8BC29F6E6BDB8003F
F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E
F96C481CBB0D6E7BDA49C6D68CFDB1D284354961534EDEEDA854C672B48A8D6B7146F90BDACB
```

```
15CE8D5DB0BAC3BCBB1FA69F2E672CC54EFBEC7684DA792F3CBF8B007A9FEA1D16374560DFA5
2F1A9C8B8AA163BBB84FF799A0954B232C279C5E9EE42505955288EAD28685A2BC0713C7745
88984846080D639C9A4EC394E53BA616D550B2B3AD691942EA2CCD33AA5B9340FD1A8FF40E9A
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69
D527959A7BC728CB272A0DB683B547F079C98012201A48DD2792B84604E8BC29F6E6BDB8003F
F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E
F96C481CBB0D6E7BDA49C6D68CFDB1D284354961534EDEEDA854C672B48A8D6B7146F90BDACB
```

There are almost certainly more affiliates involved in this group, however, based on our current locker visibility, we can confidently confirm **29 discovered campaigns and ransomware samples**.

Plain text

Copy to clipboard

Open code in new window

EnlighterJS 3 Syntax Highlighter

```
CmpID: 03860d116701cdc9d9bf9c45099bb3d3 TOX:
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69

CmpID: 11e7baca7e652995b2364fdab0d362b7 TOX:
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3

CmpID: 2cd4eb358c45ca783a20ec854a5a860c TOX:
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3
```

CmpID: 2e5d1a352885a6efd84dbc0387cbc79e TOX:  
D527959A7BC728CB272A0DB683B547F079C98012201A48DD2792B84604E8BC29F6E6BDB8003F

CmpID: 3b7b4f2d33bdfb8a31b480d0eb2815cd TOX:  
F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E

CmpID: 4a94d2b730a5a63e6cd54a9b0bb4ea71 TOX:  
F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E

CmpID: 4e0c37cbf4dde9683943c8a738e5b00a TOX:  
D527959A7BC728CB272A0DB683B547F079C98012201A48DD2792B84604E8BC29F6E6BDB8003F

CmpID: 51dec3e170f8a181cc9aea8dcc90c7ab TOX:  
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69

CmpID: 583fe1c1a39f6b873a5c0997bea1f657 TOX:  
15CE8D5DB0BAC3BCBB1FA69F2E672CC54EFBEC7684DA792F3CBF8B007A9FEA1D16374560DFA5

CmpID: 697f182826495662427ca49edbb345fc TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3

CmpID: 71d503709af88821c183a1d0b7ae06ec TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3

CmpID: 721606b3659f2c2d80a196ed3cd60053 TOX:  
F96C481CBB0D6E7BDA49C6D68CFDB1D284354961534EDEEDA854C672B48A8D6B7146F90BDACB

CmpID: 735069890a414869f0113de820ba9afb TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3

CmpID: 74ea100b581ec32ea6c2ac2a0030a9f6 TOX:  
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69

CmpID: 776e86c13433747299a4e5f9f22e3415 TOX:  
2F1A9C8B8AA163BBB84FF799A0954B232C279C5E9EE42505955288EAAD28685A2BC0713C7745

CmpID: 7aae8fd9187c88dd0292cce1abd050e2 TOX:  
F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E

CmpID: 82160a7da5fc4c935e6f48d38a5aaaa6 TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3

CmpID: 893f735e9a8cc9814dc6eccd5579561c TOX:  
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69

CmpID: 8fcee4fd9ce32dd620ccd580297c7c5 TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3

CmpID: 92d8bd2a6ee7f6d5c84e037066ce0539 TOX:  
2F1A9C8B8AA163BBB84FF799A0954B232C279C5E9EE42505955288EAAD28685A2BC0713C7745

CmpID: a023a6b15419600dc3f6b93e11761dfe TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3

CmpID: a73526d89e5fb7b57f50d8da340e53e9 TOX:  
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69

CmpID: abd11823ddcc3d746ad8621e677a93eb TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3

CmpID: b5b42ac289581b3387ebf120129a19a6 TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3

CmpID: b68e019efb39b85f5a0326e22fd4498a TOX:  
F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E

CmpID: bc6b87c79bc71a78da623d031ec1a958 TOX:  
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69

CmpID: d75246d230f22b1da6bbf5fceed2ef2 TOX:  
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69

CmpID: da9cff1b478b64d47b68d50330e96c60 TOX:  
D527959A7BC728CB272A0DB683B547F079C98012201A48DD2792B84604E8BC29F6E6BDB8003F

CmpID: ead0d7a8ae0a6ffb7f0a5873fec4ff5e TOX:  
88984846080D639C9A4EC394E53BA616D550B2B3AD691942EA2CCD33AA5B9340FD1A8FF40E9A

CmpID: 03860d116701cdc9d9bf9c45099bb3d3 TOX:  
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69 CmpID:  
11e7baca7e652995b2364fdb0d362b7 TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3 CmpID:  
2cd4eb358c45ca783a20ec854a5a860c TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3 CmpID:  
2e5d1a352885a6efd84dbc0387cbc79e TOX:  
D527959A7BC728CB272A0DB683B547F079C98012201A48DD2792B84604E8BC29F6E6BDB8003F CmpID:  
3b7b4f2d33bdfb8a31b480d0eb2815cd TOX:  
F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E CmpID:  
4a94d2b730a5a63e6cd54a9b0bb4ea71 TOX:  
F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E CmpID:  
4e0c37cbf4dde9683943c8a738e5b00a TOX:  
D527959A7BC728CB272A0DB683B547F079C98012201A48DD2792B84604E8BC29F6E6BDB8003F CmpID:  
51dec3e170f8a181cc9aea8dcc90c7ab TOX:  
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69 CmpID:  
583fe1c1a39f6b873a5c0997bea1f657 TOX:  
15CE8D5DB0BAC3BCBB1FA69F2E672CC54EFBEC7684DA792F3CBF8B007A9FEA1D16374560DFA5 CmpID:  
697f182826495662427ca49edbb345fc TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3 CmpID:  
71d503709af88821c183a1d0b7ae06ec TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3 CmpID:  
721606b3659f2c2d80a196ed3cd60053 TOX:  
F96C481CBB0D6E7BDA49C6D68CFDB1D284354961534EDEEDA854C672B48A8D6B7146F90BDACB CmpID:  
735069890a414869f0113de820ba9afb TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3 CmpID:  
74ea100b581ec32ea6c2ac2a0030a9f6 TOX:  
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69 CmpID:  
776e86c13433747299a4e5f9f22e3415 TOX:  
2F1A9C8B8AA163BBB84FF799A0954B232C279C5E9EE42505955288EAAD28685A2BC0713C7745 CmpID:  
7aae8fd9187c88dd0292cce1abd050e2 TOX:  
F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E CmpID:  
82160a7da5fc4c935e6f48d38a5aaaa6 TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3 CmpID:  
893f735e9a8cc9814dc6eccd5579561c TOX:  
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69 CmpID:  
8fcee4fd9ce32dd620ccd580297c7c5 TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3 CmpID:  
92d8bd2a6ee7f6d5c84e037066ce0539 TOX:  
2F1A9C8B8AA163BBB84FF799A0954B232C279C5E9EE42505955288EAAD28685A2BC0713C7745 CmpID:  
a023a6b15419600dc3f6b93e11761dfe TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3 CmpID:  
a73526d89e5fb7b57f50d8da340e53e9 TOX:

D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69 CmpID:  
abd11823ddcc3d746ad8621e677a93eb TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3 CmpID:  
b5b42ac289581b3387ebf120129a19a6 TOX:  
98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3 CmpID:  
b68e019efb39b85f5a0326e22fd4498a TOX:  
F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E CmpID:  
bc6b87c79bc71a78da623d031ec1a958 TOX:  
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69 CmpID:  
d75246d230f22b1da6bbf5fceed2ef2 TOX:  
D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69 CmpID:  
da9cff1b478b64d47b68d50330e96c60 TOX:  
D527959A7BC728CB272A0DB683B547F079C98012201A48DD2792B84604E8BC29F6E6BDB8003F CmpID:  
ead0d7a8ae0a6fffb7f0a5873fec4ff5e TOX:  
88984846080D639C9A4EC394E53BA616D550B2B3AD691942EA2CCD33AA5B9340FD1A8FF40E9A

CmpID: 03860d116701cdc9d9bf9c45099bb3d3 TOX: D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69  
CmpID: 11e7baca7e652995b2364fdab0d362b7 TOX: 98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3  
CmpID: 2cd4eb358c45ca783a20ec854a5a860c TOX: 98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3  
CmpID: 2e5d1a352885a6efd84dbc0387cbc79e TOX: D527959A7BC728CB272A0DB683B547F079C98012201A48DD2792B84604E8BC29F6E6BDB8003F  
CmpID: 3b7b4fd2d33bdfb8a31b480d0eb2815cd TOX: F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E  
CmpID: 4a94d2b730a5a63e6cd54a9b0bb4ea71 TOX: F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E  
CmpID: 4e0c37cbf4dde9683943c8a738e5b00a TOX: D527959A7BC728CB272A0DB683B547F079C98012201A48DD2792B84604E8BC29F6E6BDB8003F  
CmpID: 51dec3e170f8a181cc9aea8dcc90c7ab TOX: D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69  
CmpID: 583fe1c1a39f6b873a5c0997bea1f657 TOX: 15CE8D5DB0BAC3BCB1FA69F2E672CC54EFBEC7684DA792F3CBF8B007A9FEA1D7A8A8D06B  
CmpID: 697f182826495662427ca49edbb345fc TOX: 98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3  
CmpID: 71d503709af88821c183a1d0b7ae06ec TOX: 98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3  
CmpID: 721606b3659f2c2d80a196ed3cd60053 TOX: F96C481CBB0D6E7BDA49C6D68CFDB1D284354961534EDEDAA854C672B48A8D06B  
CmpID: 735069890a414869f0113de820ba9afb TOX: 98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3  
CmpID: 74ea100b581ec32ea6c2ac2a0030a9f6 TOX: D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69  
CmpID: 776e86c1343747299a4e5f9f22e3415 TOX: 2F1A9C888AA163BBB84FF799A0954B232C279C5E9EE42505955288EAAAD28685A  
CmpID: 7aae8fd9187c88dd0292cce1abd050e2 TOX: F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E  
CmpID: 82160a7da5fc4c935e6f48d38a5aaaa6 TOX: 98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3  
CmpID: 893f735e9a8cc9814dc6eccd5579561c TOX: D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69  
CmpID: 8fceeaa4fd9ce32dd620ccd580297c7c5 TOX: 98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3  
CmpID: 92d8bd2a6ee7f6d5c84e037066ce0539 TOX: 2F1A9C888AA163BBB84FF799A0954B232C279C5E9EE42505955288EAAAD28685A  
CmpID: a023a6b15419600dc3f6b93e11761dfe TOX: 98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3  
CmpID: a73526d89e5fb7b57f50d8da340e53e9 TOX: D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69  
CmpID: abd11823ddcc3d746ad8621e677a93eb TOX: 98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3  
CmpID: b5b42ac289581b3387ebf120129a19a6 TOX: 98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3  
CmpID: b68e019efb39b85f5a0326e22fd4498a TOX: F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E  
CmpID: bc6b87c79bc71a78da623d031ec1a958 TOX: D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69  
CmpID: d75246d230f22b1da6bbf5fceed2ef2 TOX: D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69  
CmpID: da9cff1b478b64d47b68d50330e96c60 TOX: D527959A7BC728CB272A0DB683B547F079C98012201A48DD2792B84604E8BC29F6E6BDB8003F  
CmpID: ead0d7a8ae0a6fffb7f0a5873fec4ff5e TOX: 88984846080D639C9A4EC394E53BA616D550B2B3AD691942EA2CCD33AA5B9340FD1A8FF40E9A

Based on this small collection of samples, most of the campaigns appear to have been conducted by the affiliate using the TOX ID `98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3` . It is also noteworthy that the RaaS administrator's TOX ID has been observed in four unique infections. This suggests that the administrator not only manages the RaaS program but also actively participates in, or directly carries out, some of the infections.

## RaaS Leak

On May 4th, 2026, on an underground forum, the RaaS administrator published a post acknowledging the claims of an internal leak involving their so-called **Rocket** database, an internal backend system used to store operational data, and addressed his affiliates directly about the incident.



Figure 6 — The Gentlemen RaaS post.

The message continues in a dismissive tone toward the leak seller and then shifts focus back to “more interesting” topics. These include a full overhaul of the communication structure, the deployment of a new NAS with unlimited storage, and several technical upgrades to the locker, such as removing hardware breakpoints, performing NTDLL unhooking, and patching ETW to suppress Event Tracing for Windows.

#### **Demanding ransom from a RaaS**

On May 5th, 2026, the account `n7778` with TOX ID

`7862AE03A73AAC2994A61DF1F635347F2D1731A77CACC155594C6B681D201F7AD6817AD3AB0A` advertised the sale of The Gentlemen’s hacked data on underground forums for 10,000 USD, payable in Bitcoin.



Figure 7 — Account selling The Gentlemen RaaS Data.

In the following days, the same account posted two MediaFire links containing proof files supporting the claimed leak.



Figure 8 — Partial leaks.

The first leaked data is a text file that contains the contents of the `shadow` file from The Gentlemen's server, including user account entries and their password hashes. The file lists many usernames, among them `zeta88` , `3NT3R` , `B1d3n` , `C0CA` , `d0wnloAd1` , `equal1z3r` , `F3N1X` , `Gblog88` , `JLL` , `LDW` , `n0n3` , `PRTGRS` , `W1Z` . Notably, we again see the `zeta88` account, the same handle that was used in the initial underground post advertising the `RaaS` program, further linking this server to the RaaS administrator.



Figure 9 — shadow file content.

The second leaked data set contains partial conversations between the RaaS operators and their affiliates across several internal channels (such as `INFO` , `general` , `TOOLS` , and `PODBOR` ). In these chats, they coordinate ongoing intrusions, exchange toolsets and EDR-kill packages, discuss infrastructure and backend components, review CVEs and exploit paths, and talk about specific victims, campaigns, and payouts.

While the partial leaked data that we obtained is around **44.4 MB**, a screenshot shared by the same account on another underground forum shows a total size of approximately **16.22 GB**, which likely corresponds to the full leaked data set.



Figure 10 — Full leaked data screenshot.

### Roles & Structure

The group appears to have a clear division of roles and responsibilities. At the core, the main operator and developer, **zeta88** (most likely **hastalamuerte**), runs the infrastructure and builds and maintains the custom ransomware locker, the RaaS panel and builder (Linux with containers and a TOR front), as well as the GPO-based spread mechanism and the locker's "spread" module. This operator also curates toolsets in the **TOOLS** channel, including EDR kill kits and **ki1jalki** collections, selects targets, and assigns them to specific teams, often talking about "targets", "подбор" (selection) channels, and distributing corporate victims to groups of 2–3 people. In addition, they manage payouts and negotiations, including multi-million ransom discussions ("переговоры на 10кк").



Figure 11 — Image shared in the chats, zeta88 – Admin.

Considering our previous assessment that the RaaS administrator also runs campaigns himself (based on TOX IDs), the leaked chats reinforce this view: they show him personally deploying the locker and encrypting at least one victim's environment.



Figure 12 — zeta88 locking message.

Often, messages sent by `zeta88` appear to be copied or adapted from earlier messages made by `hastalamuerte`, and affiliates frequently mention `hastalamuerte` by name. Taken together with previous findings and earlier RaaS posts linked to `zeta88`, these patterns strongly suggest that `hastalamuerte` and `zeta88` are very likely the same person.



Figure 13 — zeta88 – hastalamuerte message.

Below this core role, key operators or affiliates such as `qbit` and `quant` handle more hands-on operational work. `qbit` is a practical operator on many cases, responsible for scanning and filtering Fortinet VPNs and other edge devices, performing reconnaissance and persistence (including “крепиться клаудом” (English: “to establish persistence via the cloud”) through Cloudflare tunnels or Zero Trust solutions), and using tools such as NetExec ( `NXC` ), RelayKing, PrivHound, and NTLM relay scanning. `qbit` frequently requests clear EDR killer sets, manuals, and guidance for locking ESXi environments, and also brings in new bot or access suppliers (“поставщик ботов”) (English: “supplier of bots”). `quant` focuses on log-based access (“логи ЛБ”, i.e. spilled credentials for OWA/O365 and similar services) and maintains a custom log parser and proprietary credential/data collector, referred to as `buildx641`, which is run from a domain-joined machine, uses `vssadmin`, shadow copies, `ntds.dit`, and `SYSTEM` copies, and collects and compresses data from multiple hosts. `quant` is oriented toward OW/OVA spam and higher-value (“тип1”) (English: “tier-1”) victims and has set up a powerful “brute server” (Threadripper PRO, 128 GB RAM, RTX 5090) for large-scale brute forcing.

Around these core and key operators, there are several other accounts, including `Wick`, `mAst3r`, `Protagor`, `Bl0ck`, `JeLLy`, `Kunder`, and `Mamba` who take on various roles such as red-teamers, advertising partners, access brokers, or case-specific collaborators; for example, `Protagor` is mentioned in connection with OV (online vault/OVA-type) spam, while `Mamba` acts as an access broker for Fortinet VPNs sourced from `ramp`.

Through this specific leak, we identified 9 unique accounts actively communicating with each other: `Kunder`, `qbit`, `JeLLy`, `Protagor`, `zeta88`, `Bl0ck`, `Wick`, `quant`, and `mAst3r`. This internal interaction pattern supports the view that these accounts form a coordinated operational network within The Gentlemen RaaS ecosystem. This number aligns with our earlier assessment based on the unique TOX IDs extracted from the ransomware lockers.

Group members collaborate on various infections and share the profits as well. As a result, the **90%** share allocated to the affiliate is often split among multiple affiliates who worked together to achieve a successful intrusion.



Figure 14 — Collaboration and profit sharing.

Based on the analyzed chat messages, the organization’s structure appears to match the model shown in the following image. It is likely that additional members exist who do not appear in this specific leak, but the roles and relationships we observe here are consistent across the available data. There are also indications of an internal separation between trusted members and newcomers—for example, one message notes that “*that Rocket is still alive – there are rookies there*”—suggesting a tiered or layered structure within the group.



Figure 15 — Organization diagram.

### Operational workflow

The conversations from the leak show a fairly standard but well-organized operational workflow. The group claims to usually gain initial access through exposed edge devices such as VPN appliances, firewalls, and other internet-facing systems, with a particular focus on platforms like Fortinet FortiGate and Cisco. They combine different methods to achieve this, including credential brute-forcing against web or VPN panels, exploiting known vulnerabilities, and buying access from third-party “bot” or access brokers. Screenshots shared in the chats also show them searching for accounts and credentials in data-breach search engines. Once they obtain a foothold, they treat these systems as pivots to move deeper into the internal network.



Figure 16 — Searching credentials & accounts.

After gaining access, the operators perform internal reconnaissance and privilege escalation to understand the environment and obtain higher-level permissions, often aiming for domain administrator access. They rely on a mixture of Active Directory discovery, certificate abuse, and various local privilege escalation techniques. At the same time, they invest significant effort into disabling or bypassing security tools such as EDR and antivirus solutions, using a combination of misconfigurations, registry abuse, logging mechanisms, and bring-your-own-vulnerable-driver-style (BYOD) techniques to tamper with or overwrite security binaries.

With elevated access and reduced defensive visibility, the group focuses on expanding across the network and preparing for the final stages of the attack. This includes lateral movement, establishing additional tunnels or proxies for reliable connectivity, and relaxing security settings to make further operations easier. They also harvest credentials and browser-based sessions to reuse existing access to corporate services. Data exfiltration is then carried out using automated tools and tuned configurations to move large volumes of data efficiently, often targeting NAS devices, backup systems, and virtualization infrastructure. Finally, once the environment is prepared and critical data is in their control, they deploy their custom ransomware “locker,” which is designed to spread quickly across the network, leverage existing administrator sessions, and encrypt systems in a coordinated manner.

Tools & Infra

The leaked conversations show that The Gentlemen RaaS operators use a repeatable and fairly mature toolset to support their operations. For remote access and C2, they rely on frameworks like ZeroPulse and Velociraptor, combined with Cloudflare-based tunnels and custom VPN setups to keep stable access into compromised networks. For offensive operations, they use a range of red-team utilities such as NetExec, RelayKing, TaskHound, PrivHound, CertiHound, and others to perform Active Directory discovery, certificate abuse, privilege escalation, and file share discovery. A separate group of tools is dedicated to EDR and AV evasion, including EDRStartupHinder, gfreeze, glinker, and DumpBrowserSecrets, as well as techniques inspired by public research on abusing Windows logging and Event Tracing for Windows (ETW). Finally, they support these activities with infrastructure and helper tools like port scanners (gogo.exe), usage guides, OSINT extensions, and password-cracking services, which together give them a reusable framework for running repeated intrusions and ransomware deployments.

| Category           | Tool / Resource | Purpose / Usage                                                 | Reference / Notes                                                                     |
|--------------------|-----------------|-----------------------------------------------------------------|---------------------------------------------------------------------------------------|
| C2 / Remote Access | ZeroPulse       | Remote access / C2 framework for controlling compromised hosts. | <a href="https://github.com/jxroot/ZeroPulse">https://github.com/jxroot/ZeroPulse</a> |
| C2 / Remote        | Velociraptor    | Used as a covert C2 platform,                                   | Often used with signed builds to reduce detection.                                    |

| Category             | Tool / Resource                 | Purpose / Usage                                                            | Reference / Notes                                                                                                           |
|----------------------|---------------------------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Access               |                                 | including memory and LSASS dumping.                                        |                                                                                                                             |
| C2 / Remote Access   | Cloudflare Zero Trust / Tunnels | Provides stealthy tunnels into victim networks over HTTPS.                 | Used together with custom VPN setups.                                                                                       |
| VPN / Network Access | wireguard-install               | Automates WireGuard VPN deployment.                                        | <a href="https://github.com/angristan/wireguard-install">https://github.com/angristan/wireguard-install</a>                 |
| VPN / Network Access | openvpn-install                 | Automates OpenVPN server setup.                                            | <a href="https://github.com/angristan/openvpn-install">https://github.com/angristan/openvpn-install</a>                     |
| VPN / Network Access | Double-VPN-with-OpenVPN         | Configures double-layer OpenVPN routing.                                   | <a href="https://github.com/pizdatiigus/Double-VPN-with-OpenVPN">https://github.com/pizdatiigus/Double-VPN-with-OpenVPN</a> |
| Offensive / Red-Team | NetExec ( NXC )                 | Multi-purpose offensive framework for AD, SMB, WinRM, and more.            | Internal usage guide via a shared NXC gist.                                                                                 |
| Offensive / Red-Team | TaskHound                       | Task and privilege abuse / persistence helper.                             | Used post-exploitation.                                                                                                     |
| Offensive / Red-Team | PrivHound                       | Identifies local privilege escalation paths and persistence opportunities. | Integrates with BloodHound data.                                                                                            |
| Offensive / Red-Team | RelayKing-Depth                 | Finds and exploits NTLM relay paths across protocols.                      | <a href="https://github.com/depthsecurity/RelayKing-Depth">https://github.com/depthsecurity/RelayKing-Depth</a>             |
| Offensive / Red-Team | CertiHound                      | Enumerates and detects ADCS misconfigurations (ESC1–ESC17).                | Used via NetExec integration.                                                                                               |
| Offensive / Red-Team | Titanis                         | Offensive tooling for Windows logging / ETW manipulation.                  | <a href="https://github.com/trustedsec/Titanis">https://github.com/trustedsec/Titanis</a>                                   |
| Offensive / Red-Team | MANSPIDER                       | Searches file shares for sensitive strings and documents.                  | Used for locating valuable data.                                                                                            |
| Offensive /          | PowerZure                       | Abuses Azure / cloud                                                       | Used for cloud-side access and escalation.                                                                                  |

| Category             | Tool / Resource             | Purpose / Usage                                                        | Reference / Notes                                                                                                                       |
|----------------------|-----------------------------|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Red-Team             |                             | misconfigurations.                                                     |                                                                                                                                         |
| Offensive / Red-Team | RegPwn                      | Registry-based privilege escalation and service abuse.                 | Often used for MSI service abuse.                                                                                                       |
| Offensive / Red-Team | Ks1Dump                     | Dumps Kerberos / LSASS-related material.                               | Used for credential theft.                                                                                                              |
| Offensive / Red-Team | Ks1Katz                     | Kerberos / LSASS post-exploitation tool similar to credential dumpers. | Complements Ks1Dump .                                                                                                                   |
| EDR / AV Evasion     | EDRStartupHinder            | Blocks or delays EDR processes at startup.                             | Based on the EDR-Startup-Process-Blocker concept.                                                                                       |
| EDR / AV Evasion     | gfreeze                     | Part of their EDR “killer” toolkit to hinder security products.        | Derived from EDR-blocking research/code.                                                                                                |
| EDR / AV Evasion     | glinker                     | Another component in their EDR evasion sets.                           | Often grouped with gfreeze .                                                                                                            |
| EDR / AV Evasion     | DumpBrowserSecrets          | Dumps browser cookies and secrets for session hijacking.               | Used to reuse corporate web sessions.                                                                                                   |
| EDR / AV Evasion     | zerosalarium ETW/log tricks | Public research they follow for ETW and log-based EDR kill techniques. | Multiple posts referenced for inspiration.                                                                                              |
| Infra / Scanning     | gogo.exe                    | Scanner for common ports and exposed services.                         | Used in early discovery phases.                                                                                                         |
| Infra / Scanning     | NXC usage gist              | Internal guide for effective NetExec usage.                            | <a href="https://gist.github.com/gitgotgitgotit/81a578e065da1ccd8c81a">https://gist.github.com/gitgotgitgotit/81a578e065da1ccd8c81a</a> |
| OSINT / Helper Tools | Sputnik browser extension   | OSINT aggregation extension to support recon.                          | Helps enrich target information.                                                                                                        |
| OSINT / Helper Tools | chamd5.org                  | Online password hash cracking service.                                 | Used for recovering cleartext passwords.                                                                                                |

| Category                   | Tool / Resource  | Purpose / Usage                            | Reference / Notes                   |
|----------------------------|------------------|--------------------------------------------|-------------------------------------|
| OSINT /<br>Helper<br>Tools | hashcracking_bot | Bot-based<br>password cracking<br>service. | Complements other cracking methods. |

The leaked chats show that the group pays close attention to other ransomware operations, including the leaked Black Basta negotiations. In particular, they discuss Black Basta’s approach to code signing and note how that group allegedly used VirusTotal to search for legitimate code-signing certificates, which were then targeted for **brute-force attacks** on their private keys. The Gentlemen actors refer to this technique as a model they can reuse or adapt, highlighting their interest in abusing trusted certificates to make their binaries look legitimate and harder to detect.



Figure 17 — Code signing conversations.

**AI mentions**

The Gentlemen mention AI usage in multiple channels and for various purposes. While it is clear that they have already used AI for code-assisted development, including experiments with Chinese models, more advanced use cases—such as locally deploying models to analyze large volumes of exfiltrated victim data—are only discussed at a conceptual level. These ideas are suggested in the chats but do not appear to be fully implemented.

zeta88 states that he built the GLOCKER admin panel in three days using AI-assisted coding. He is candid about the limitations of this approach, noting that while AI can speed up development, you still need to understand what you are doing and be able to guide and correct the code it produces.



Figure 18 — zeta88 “vibe-coded” the Panel.

Members share their AI preferences across different chats. zeta88 states that he finds **DeepSeek**, **Qwen**, **Kimi**, and **Emi** the most effective models for his purposes, particularly for coding assistance and technical queries.



Figure 19 — AI preferences.

He also suggests adding more Chinese LLMs to their toolkit, in addition to those they are already considering or using, such as **DeepSeek** and **Qwen**.



Figure 20 — Chinese LLMs suggestions.

A couple of months later, qbit shares in the INFO channel their recommendation for “the most radical neural network, which creates any content without censorship. Runs on Qwen 3.5 with all barriers removed... Zero refusals. Absolutely no restrictions.”



Figure 21 — Qwen 3.5 post.

zeta88 directs affiliates to use AI as a quick reference—for example, to look up FortiGate internals—rather than asking in the channel.



Figure 22 — Usage of AI as quick reference.

For more challenging tasks such as operational data analysis, identifying high-value access points, and offloading much of the manual data-triage work to an AI model, the operators explicitly discuss using an uncensored, self-hosted LLM.

However these suggestions appear to remain theoretical, as **Protagor** admits, *“I have no idea how to do that, but I think it’s possible.”*



Figure 23 — Local, self-hosted LLM.

Screenshot shared in the chats shows an LLM response on how to send an email to all users via the Jira admin interface, in **Russian**. It describes two methods, mainly using Jira Automation and user groups.



Figure 24 — Screenshot shared in the chats.

The group appears to be experimenting with well-known Chinese LLMs and has considered using locally hosted models to assist with data triage on stolen information.

### CVEs and Exploits

While the group discusses these vulnerabilities, shares related links, and occasionally attempts to exploit specific systems using particular CVEs, we cannot confirm whether the targeted machines were actually vulnerable to the exact vulnerabilities they referenced.

- **CVE-2024-55591 – FortiOS management interface**

This vulnerability affects the FortiOS management interface and fits directly into their broader focus on Fortinet appliances as high-value initial access points. While the chats do not show detailed exploitation steps, the presence of this CVE alongside their FortiGate targeting suggests it is part of the set of vulnerabilities they track for potential use against exposed management interfaces.



Figure 25 — CVE-2024-55591, related message.

- **CVE-2025-32433 – Erlang SSH vulnerability (Cisco context)**

In the logs, `qbit` shares a proof-of-concept (PoC) for `CVE-2025-32433`, and `zeta88` comments on its quality and applicability. This shows that the group is not simply aware of the CVE but is actively evaluating whether it can be used in real operations, specifically in environments where Cisco or Erlang-based SSH services are exposed. Even if they are cautious about PoC reliability, the discussion confirms that this vulnerability is part of their potential exploit toolkit.



Figure 26 — qbit & zeta88 related posts.

- CVE-2025-33073 – NTLM reflection / NTLM relay

qbit references RelayKing and shares output showing domains being scanned for NTLM relay issues, including checks that explicitly cover CVE-2025-33073. This is strong evidence that they are not just reading about the vulnerability but have integrated RelayKing into their standard reconnaissance process to generate target lists for tools like ntlmrelayx. In other words, CVE-2025-33073 is a vulnerability they actively scan for and intend to exploit as part of broader NTLM relay workflows.



Figure 27 — Mention of CVE-2025-33073.

- **Other Exploit Paths (Without Explicit CVE IDs)**

The operators also make heavy use of technique-based exploits where no specific CVE number is mentioned in the chats. These include:

- **MSI service abuse via RegPwn**, used for privilege escalation.
- **Veeam to domain admin paths**, based on public write-ups about misconfigured backup infrastructure.
- **iDRAC to domain admin paths**, leveraging Dell iDRAC weaknesses.
- **WPR, AutoLogger, and ETW manipulation** techniques documented by zerosalarium and others to overwrite or disable security binaries.

### Payments & Negotiations

Zeta88 acts as the organizer/administrator, distributing cryptocurrency payouts to team members (including those who are “AFK”) and advising on how to cash out proceeds via Bitcoin wallets (Guarda, Trust Wallet, Exodus). The group discusses AML (Anti-Money Laundering) evasion strategies. Zeta88 sends a BTC transaction to Kunder as a payout, which Kunder confirms receiving.



Figure 28 — Transaction link shared.

The specific mentions of how they handle Bitcoin laundering/cash out:

1. **Exchange Chains (“связки обмена”)** Zeta88 mentions running ~800 transactions through “buy desks” (скупов) via exchange chains, or sometimes sending directly, suggesting chain-hopping to obscure transaction origins.
2. **AML Checking** They discuss whether their BTC is “clean” and reference a buyer who actively checks AML scores before transacting. They’re uncertain how the scoring works but are aware their coins could be traced.
3. **Tinkoff QR Code Cash-Out** A specific method mentioned: a buyer converts BTC to cash via **Tinkoff bank QR codes**, with minimums of 400k rubles (previously 250k). This converts crypto directly to Russian banking infrastructure.
4. **Physical Cash Delivery** Kunder mentions “**locking in the rate**” and a guy physically bringing cash at the end of the month, a classic peer-to-peer OTC (over-the-counter) arrangement that bypasses exchanges entirely.
5. **Wallet Infrastructure** They recommend non-custodial wallets (Guarda, Trust Wallet, Exodus) specifically to avoid KYC/AML controls that centralized exchanges enforce.

Blurry screenshots from the leak also shed light on the **financial side** of the operation. Although not fully legible, they appear to show a negotiation where the group secured approximately **190,000 USD** after a discount of about **60,000 USD** from the initial ransom demand.



Figure 29 — Agreement to pay 190,000 USD.

zeta88 is very aware of the importance of maximizing pressure on extorted victims to increase the chances of payment. In his private channel, he drafts a generic follow-up letter that can be adapted to any company, emphasizing the costs of not paying the ransom, including regulatory exposure, reputational damage, and operational impact, and citing assessments from

previous attacks. This is not the standard ransom note deployed alongside the encryption, but an additional, more tailored communication intended to reinforce the pressure on the victim.



Figure 30 — Negotiation playbook.

### Interesting Negotiation Case

In a high-profile attack in April 2026, a **software consultancy company from United Kingdom** publicly reported a breach. The company’s leadership stated in an open letter that only “typical business data, including business contact information, contracts, and NDAs related to client work” had been accessed.

From what appears to be a personal channel used by **zeta88**, he drafts a ransom demand letter addressed to the UK company, detailing what The Gentlemen claim to have exfiltrated, including customer infrastructure data, secrets, OAuth credentials, and more. The letter explicitly emphasizes potential **GDPR** violations as leverage to pressure the victim into paying.



Figure 31 — Ransom note.

Two weeks later, the group published the consultancy's identity and breach details on their data leak site (**DLS**). According to the internal chats, data exfiltrated from the consultancy was then reused **both before and during** attacks against a company in Turkey, where The Gentlemen gained initial access via a vulnerable VPN appliance.



Figure 32 — Forti access to company in Turkey.

zeta88 ran this operation alongside Protagor, creating a backdoor Okta service account himself—typical of his intensive, hands-on involvement in many of the intrusions documented in the leaked discussions. During the same campaign, zeta88 explicitly references data from the UK consultancy breach to cross-reference and enrich information about the Turkish company, illustrating how prior compromises are used to enrich and support new attacks.



Figure 33 — UK company containing information for Turkish company.

One example mentioned was an internal “**Transfer/Migration Document**” (in the local language), an internal project document the consultancy maintained in its own collaboration platform describing work they did for the company in Turkey. This document, stolen in the first breach, was then used in the second.

The group discussed how best to use this access for extortion. In their internal chats, they talked about publishing the company from Turkey on their DLS together with a statement that, The access to the company in Turkey was obtained through the **compromised consultancy from United Kingdom**.



Figure 34 — DLS statement discussions.

This served a dual purpose:

1. **Punishing the consultancy (UK)**, which the actors described as “a very bad company.”
2. **Increasing pressure on the company in Turkey**, by promising to show exactly how they gained access so that, the Turkish would be encouraged to **legally pursue** the consultancy in UK.



Figure 35 — Initial access proof.

Eventually, the Turkish company was published on the group's DLS, and the attackers "credited" the **consultancy in UK** as their "access broker".

#### Their View of Other RaaS Programs and Actors

The actors consistently frame the RaaS ecosystem through the lenses of **brand strength**, **payout reliability**, and **affiliate leverage** (percentage splits and control over negotiations). Among the programs mentioned, they clearly distinguish a small "top tier" from a broader landscape of lesser or untrusted players.

| Program / Group   | Things Discussed                                                                                                                                                                      | Subjective Sentiment (Their View)                                                                |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| HelloKitty        | Name/brand as something they'd like to use; jokes about linking to the real Hello Kitty site and putting (R) everywhere; described explicitly as a "мощный бренд".                    | Very positive on brand strength and recognition; sees it as a powerful marketing asset.          |
| Kraken            | Mention that "товарищи кракен" wrote to qbit ; qbit later says their team might "move" over to zeta88 's side.                                                                        | Neutral-pragmatic; current or past orbit, but clearly willing to switch away for better options. |
| Dragon Force      | One of only two programs zeta88 would choose from "all presented"; explicitly says they pay both operators and adverts; only negative comments heard were about their software/panel. | Strongly positive overall; trusted, in the top tier of programs they respect.                    |
| Gunra             | Listed among candidate PPs for a supplier; zeta88 says "че эт ваще такое...", and lumps it with Hyflock ; calls the operator "этот мудень".                                           | Negative; unserious / low-relevance; clear disdain for the operator.                             |
| Hyflock           | Same context as Gunra ; zeta88 dismisses it in the same breath as Gunra , with the same derogatory comment about the person behind it.                                                | Negative; grouped with Gunra as not to be taken seriously.                                       |
| ShadowByt3\$ RAAS | Appears in the candidate list; zeta88 simply comments "хэ" (doesn't know).                                                                                                            | Neutral; no formed opinion, neither trust nor distrust expressed.                                |
| Anubis            | Appears in the candidate list; zeta88 asks "% видел он?", focusing on what                                                                                                            | Cautious / skeptical; interest hinges on profit split; no clear                                  |

| Program / Group              | Things Discussed                                                                                                                                                                                                                       | Subjective Sentiment (Their View)                                                                              |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
|                              | percentage they take.                                                                                                                                                                                                                  | positive trust.                                                                                                |
| CHAOS                        | Appears in the candidate list; zeta88 asks whether they will still take that supplier (“возьмут ли они его еще”).                                                                                                                      | Uncertain; doubts about acceptance / relationship continuity; not a clearly preferred option.                  |
| LockBit (tooling)            | quant asks what a локбит тулза actually is (builder or decryptor), notes he has not opened it; no explicit evaluation of the group itself.                                                                                             | Curious but cautious; tooling is not trusted or fully understood yet; no explicit sentiment on LockBit group.  |
| Black Basta / Devman         | quant asks if “блек баста это девман”; zeta88 speaks harshly about “David” and his link to Devman , calls him “мудак” and “чепуха”, wishes them невыплат (non-payment).                                                                | Strongly negative but personalized; animosity toward David / Devman rather than a structured view of the RaaS. |
| “Red team” / Mr Beng cluster | Mentions Редтим=красный лотос=арсен=баламут=студент and “мистер БЕИГ”; mocks offer of 15k for “source code” of a C2 built on top of white tools ( Velociraptor , etc.); ridicules this as overpriced and based on legitimate software. | Negative; sees them as overpriced grifters repackaging white tools with heavy marketing.                       |

Conclusion

The Gentlemen **RaaS** program has quickly evolved into a highly active and structured ransomware ecosystem. With over **320 public victims** in 2026 and hundreds more systems visible through related infrastructure, it stands among the most productive RaaS operations that maintain a public data-leak presence. The leaked **Rocket** backend and internal chats show that this scale is driven not by a loose crowd, but by a **small, tightly coordinated core** of about **9 named operators** and at least **8 distinct affiliate TOX IDs**, all organized around the administrator **zeta88 / hastalamuerte**, who both runs the platform and participates directly in operations.

The leak reveals a repeatable, human-operated ransomware playbook: initial access through exposed edge infrastructure (such as VPNs and management interfaces), rapid expansion and privilege escalation, heavy investment in **EDR/AV evasion** and ETW/logging tampering, and systematic use of shared tools for discovery, lateral movement, credential theft, and data exfiltration. The group actively tracks and evaluates modern vulnerabilities, including **CVE-2024-55591**, **CVE-2025-32433**, and **CVE-2025-33073**and combines them with technique-driven paths like backup and management-controller abuse and NTLM relay workflows, giving them a flexible exploitation pipeline.

Overall, The Gentlemen exemplifies how contemporary RaaS programs blend **productized ransomware** with **professional intrusion teams**. A small, well-organized set of operators, supported by curated tooling, structured communication channels, and up-to-date exploit knowledge, can generate substantial impact in a short time. For defenders, this underscores the need to harden internet-facing services, close known misconfigurations and relay paths, and monitor for the specific tools, workflows, and TOX-based communication patterns tied to this group.

Indicators of Compromise

| Description           | Value                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The Gentlemen Windows | 025fc0976c548fb5a880c83ea3eb21a5f23c5d53c4e51e862bb893c11adf712a1334f0189a8e6dbc48456fa4b482c5726ab7609f7fa652fcc4c1a96f2334436f1af419b36a5edefef387409e2b3248c9223f7dc49a4f7b15ea095d371c3a70b222b38dad7da097ea03aa28d0614164cd25fafeb1383dbc15047e34c8050f6f6724ac3588fb8cfbff63b7fdcfbc7dec1f3c60e54e6f949dd69d68e89e0c89d9662ed9494e9b7b68415b4eb151c922c82c0191294d0aa443dd2cb5133e6bfe3d5d |

| Description         | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | 3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c9235<br>3c2182cb0bc7528829ef03f1b1745a92bcc47d917eb8870862488f21fdf1a6d6<br>48d9b2ce4fcd6854a3164ce395d7140014e0b58b77680623f3e4ca22d3a6e7fd<br>4a175eed927c0a477eafb8aa35a93c191748acaa78ac7aec8ea3c4cd868887c<br>51b9f246d6da85631131fcd1fabf0a67937d4bdde33625a44f7ee6a3a7baebd2<br>62c2c24937d67fdeb43f2c9690ab10e8bb90713af46945048db9a94a465ffcb8<br>6a3ab9e984a759d55af4e84487d1fc44683065cc9a1089d5aa4ad1c0e4e84a63<br>860a6177b055a2f5aa61470d17ec3c69da24f1cdf0a782237055cba431158923<br>87d25d0e5880b3b5cd30106853cbfc6ef1ad38966b30d9bd5b99df46098e546c<br>8aa0cb69ca2777001e0f4ba0eaab0841592710e4cc5ccd6b0b526d78bbd8bfbba<br>8c87134c1b45e990e9568f0a3899b0076f94be16d3c40fa824ac1e6c6ee892db<br>91415e0b9fe4e7cbe43ec0558a7adf89423de30d22b00b985c2e4b97e75076b1<br>994d6d1edb57f945f4284cc0163ec998861c7496d85f6d45c08657c9727186e3<br>9f61ff4deb8afced8b1ecdc8787a134c63bde632b18293fbfc94a91749e3e454<br>a7a19cab7aab606f833fa8225bc94ec9570a6666660b02cc41a63fe39ea8b0ad<br>b67958afc982cafb1c3f114b444d7f4c91a88a3e7a86f89ab8795ac2110d1e6<br>c46b5a18ab3fb5fd1c5c8288a41c75bf0170c10b5e829af89370a12c86dd10f8<br>c7f7b5a6e7d93221344e6368c7ab4abf93e162f7567e1a7bcb8786cb8a183a73<br>dce2e5cc00eff2493f8ced546dc51f9d5ef78c5ee56805906ec642dfa77a1c70<br>dfe696ff713318c53fb17731bd4a6585a02c085b590149b19847990b324a0be6<br>ec368ae0b4369b6ef0da244774995c819c63cfff7fd2132379963b9c1640ccd2<br>efaf8e7422ffd09c7f03f1a5b4e5c2cc32b05334c18d1ccb9673667f8f43108f<br>f736be55193c77af346dbe905e25f6a1dee3ec1aedca8989ad2088e4f6576b12<br>fc75ed2159e0c8274076e46a37671cfb8d677af9f586224da1713df89490a958 |
| The Gentlemen Linux | 1eece1e1ba4b96e6c784729f0608ad2939cfb67bc4236dfababbe1d09268960c<br>5dc607c8990841139768884b1b43e1403496d5a458788a1937be139594f01dca<br>788ba200f776a188c248d6c2029f00b5d34be45d4444f7cb89ffe838c39b8b19                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Yara Rule

Plain text

Copy to clipboard

Open code in new window

EnlighterJS 3 Syntax Highlighter

rule thegentlemen\_ransomware

```
{
```

```
meta:
```

```
author = "@Tera0017/Check Point Research"
```

```
description = "The Gentlemen Ransomware written in GO."
```

```
strings:
```

```
$string1 = "Silent mode (don't rename files)" ascii
```

```
$string2 = "Encrypt only mapped and UNC network shares" ascii
```

```
$string3 = "README-GENTLEMEN.txt" ascii
```

```
$string4 = "gentlemen.bmp" ascii
```

```
$string5 = "gentlemen_system" ascii
```

\$string6 = "[+] Encryption started. Going background..." ascii

\$string7 = "[+] FULL Encryption started" ascii

condition:

uint16(0) == 0x5A4D and 4 of them

}

rule thegentlemen\_ransomware { meta: author = "@Tera0017/Check Point Research" description = "The Gentlemen Ransomware written in GO." strings: \$string1 = "Silent mode (don't rename files)" ascii \$string2 = "Encrypt only mapped and UNC network shares" ascii \$string3 = "README-GENTLEMEN.txt" ascii \$string4 = "gentlemen.bmp" ascii \$string5 = "gentlemen\_system" ascii \$string6 = "[+] Encryption started. Going background..." ascii \$string7 = "[+] FULL Encryption started" ascii condition: uint16(0) == 0x5A4D and 4 of them }

```
rule thegentlemen_ransomware
{
  meta:
    author = "@Tera0017/Check Point Research"
    description = "The Gentlemen Ransomware written in GO."
  strings:
    $string1 = "Silent mode (don't rename files)" ascii
    $string2 = "Encrypt only mapped and UNC network shares" ascii
    $string3 = "README-GENTLEMEN.txt" ascii
    $string4 = "gentlemen.bmp" ascii
    $string5 = "gentlemen_system" ascii
    $string6 = "[+] Encryption started. Going background..." ascii
    $string7 = "[+] FULL Encryption started" ascii
  condition:
    uint16(0) == 0x5A4D and 4 of them
}
```

---

Source: <https://research.checkpoint.com/2026/thus-spoke-the-gentlemen/>