New FIN7-Linked Infrastructure, PowerNet Loader, and Fake Update Attacks

recordedfuture.com/research/grayalpha-uses-diverse-infection-vectors-deploy-powernet-loader-netsupport-rat

GrayAlpha Uses Diverse Infection Vectors to Deploy PowerNet Loader and NetSupport RAT

Executive Summary

Insikt Group identified new infrastructure associated with GrayAlpha, a threat actor that overlaps with the financially motivated group commonly referred to as FIN7. This newly identified infrastructure includes domains used for payload distribution and additional IP addresses believed to be tied to GrayAlpha. Insikt Group discovered a custom PowerShell loader named PowerNet, which decompresses and executes NetSupport RAT. Insikt Group identified another custom loader, referred to as MaskBat, that has similarities to FakeBat but is obfuscated and contains strings linked to GrayAlpha. Overall, Insikt Group found three primary infection methods: fake browser update pages, fake 7-Zip download sites, and the traffic distribution system (TDS) TAG-124. Notably, the use of TAG-124 had not been publicly documented prior to this report. Although all three infection vectors were observed being used simultaneously, only the fake 7-Zip download pages were still active at the time of writing, with newly registered domains appearing as recently as April 2025. Further analysis of these sites led to the identification of an individual who may be involved in the GrayAlpha operation.

In the near term, defenders are advised to enforce application allow-lists to block the download of seemingly legitimate files that contain malware. Where allow-lists are not practical, comprehensive employee security training becomes essential, particularly in recognizing suspicious behaviors such as unexpected prompts for browser updates or redirects caused by malvertising. Additionally, the use of detection rules, such as the YARA rules and Malware Intelligence Hunting queries provided in this report, is critical for identifying both existing and past infections. These rules should be updated frequently and supported with broader detection techniques, including monitoring of network artifacts and using Recorded Future Network Intelligence, due to the constantly evolving nature of malware.

Looking ahead, defenders must monitor the broader cybercriminal ecosystem to anticipate and respond to emerging threats more effectively. The continued professionalization of cybercrime increases the likelihood of organizations across multiple industries being targeted. This trend is driven by the sustained profitability of cybercrime, limited international law enforcement collaboration, and the continuous evolution of security technologies, which in turn drive innovation among threat actors. While advanced persistent threat (APT) activity is often linked to state-sponsored entities, GrayAlpha illustrates that cybercriminal groups can demonstrate a similar level of persistence. Much like the ransomware-as-a-service (RaaS) model, cybercriminals are becoming increasingly specialized and collaborative, making it imperative to adopt a comprehensive and adaptive security posture.

Key Findings

- Insikt Group has identified new infrastructure linked to GrayAlpha — a threat actor overlapping with the group commonly known as FIN7 — including domains utilized for payload distribution and additional IP addresses believed to be part of the threat actor's infrastructure.
- Insikt Group has identified a new custom PowerShell loader dubbed PowerNet that decompresses and executes NetSupport RAT.
- Insikt Group identified another custom loader, referred to as MaskBat, which has similarities to FakeBat but is obfuscated and contains strings linked to GrayAlpha.
- Insikt Group identified three main infection vectors associated with GrayAlpha: fake browser update pages, fake 7-Zip download sites, and the TDS TAG-124 network. Notably, the use of the TDS TAG-124 delivery mechanism had not been publicly documented prior to this report.
- While all three infection methods were employed simultaneously, only the fake 7-Zip download pages appear to remain active at the time of writing, with the most recent domains surfacing as recently as April 2025.
- Through the analysis of the 7-Zip pages, Insikt Group identified an individual who may be connected to the GrayAlpha operation.

Background

GrayAlpha is a threat actor cluster that overlaps with the financially motivated cybercriminal group commonly known as FIN7, sharing key infrastructure, tooling, and tradecraft.

FIN7 has been active since at least 2013 and is considered one of the most prolific and technically sophisticated cybercriminal groups targeting organizations worldwide. The group is organized like a professional business, with compartmentalized teams handling malware development, phishing operations, money laundering, and management. FIN7 is primarily known for financially motivated campaigns involving the theft of payment card data and unauthorized access to corporate networks, particularly within the retail, hospitality, and financial sectors.

In 2018, the US Department of Justice (US DOJ) unsealed indictments against three high-ranking FIN7 members — Dmytro Fedorov, Fedir Hladyr, and Andrii Kolpakov — highlighting the group's extensive operations against businesses across 47 US states and multiple countries. Operating under the name of a sham cybersecurity firm, "Combi Security," FIN7 leveraged social engineering and customized malware, including variants of Carbanak, the group's in-house developed backdoor, to compromise thousands of point-of-sale systems and exfiltrate over 15 million payment card records. The US DOJ prosecutions revealed the group's hierarchical command structure, with members fulfilling defined roles in intrusion operations, malware administration, and logistical coordination. Despite the disruption to its leadership, FIN7's underlying infrastructure and tradecraft persisted, enabling the broader criminal enterprise to continue targeting global organizations.

FIN7 uses a range of custom and repurposed malware and tooling to support its operations. The group typically gains initial access through spearphishing emails containing malicious attachments or links hosted on compromised sites, often combined with callback phishing to increase credibility. FIN7's early operations leveraged its then-proprietary Carbanak backdoor as the primary command-and-control framework, enabling the group to manage compromised hosts and coordinate post-compromise activity. POWERTRASH — a uniquely obfuscated, PowerShell-based, in-memory loader adapted from the PowerSploit framework — has also been a consistent feature of FIN7 intrusions, used to deploy payloads such as DiceLoader and cracked Core Impact implants to support exploitation, lateral movement, and persistence. FIN7 also developed AuKill (also known as AvNeutralizer), a custom EDR evasion utility designed to disable endpoint security solutions, which was later reported to have been offered for sale by the group on criminal marketplaces. In its most recent campaigns, FIN7 has been observed deploying the Python-based Anubis backdoor, which provides full system control via in-memory execution and communicates with its command-and-control infrastructure using Base64-encoded data.

In 2023, FIN7 expanded its operations to include the deployment of ransomware through affiliations with RaaS groups such as REvil and Maze, while also managing its own RaaS programs, including the now-retired Darkside and BlackMatter. More recently, FIN7 has been observed leveraging NetSupport RAT embedded within malicious MSIX application packages, delivered via fake update sites and malvertising.

Threat Analysis

Infection Vectors

Over the past year, Insikt Group has identified three distinct infection vectors associated with GrayAlpha, observed during overlapping timeframes, and all ultimately resulting in NetSupport RAT infections. These vectors include:

- **Infection Vector 1:** Fake software updates impersonating legitimate products such as Concur
- **Infection Vector 2:** Malicious 7-Zip download pages
- **Infection Vector 3:** Use of the TAG-124 TDS

In these campaigns, GrayAlpha employed two primary types of PowerShell loaders: a self-contained custom script known as PowerNet, and a dynamic loader — a customized variant of FakeBat — referred to as MaskBat (see **Figure 1**).

Figure 1: *GrayAlpha using three different infection vectors, all leading to NetSupport RAT infections (Source: Recorded Future)*

Infection Vector 1: Fake Browser Updates

Infrastructure Analysis

Since at least April 2024, GrayAlpha has been observed leveraging fake browser update websites as part of its operations. These sites impersonate a range of legitimate products and services, including Google Meet, LexisNexis, Asana, AIMP, SAP Concur, CNN, the Wall Street Journal, and Advanced IP Scanner, among others. **Table 1** provides a list of domains associated with Infection Vector 1 that were still resolving as of 2025. However, it is important to note that active domain resolution does not necessarily indicate ongoing use by threat actors; in fact, the most recently observed domain began resolving in September 2024. A comprehensive list of all domains linked to Infection Vector 1 — including those that did not resolve at any point in 2025 — can be found in **Appendix A**.

Domain

IP Address

ASN

First Seen	Last Seen
2024-aimp[.]info	
86[.]104[.]72[.]23	
AS44477	
2024-07-04	
2025-05-04	
advanced-ip-scanner[.]link	
138[.]124[.]183[.]79	
AS44477	
2024-04-29	
2025-04-30	
aimp[.]day	
138[.]124[.]183[.]176	
AS44477	
2024-04-10	
2025-04-11	
aimp[.]pm	
138[.]124[.]183[.]176	
AS44477	
2024-04-22	
2025-04-23	
aimp[.]xyz	
38[.]180[.]142[.]198	
AS29802	
2024-05-08	
2025-05-02	
concur[.]life	
103[.]35[.]191[.]222	
AS44477	
2024-05-07	
2025-05-04	
law2024[.]info	
91[.]228[.]10[.]81	
AS44477	
2024-06-12	
2025-05-04	

law2024[.]top

91[.]228[.]10[.]81

AS44477

2024-06-13

2025-05-05

lexis2024[.]info

103[.]35[.]191[.]137

AS44477

2024-06-10

2025-05-05

lexis2024[.]pro

103[.]35[.]191[.]137

AS44477

2024-06-11

2025-05-03

lexisnex[.]pro

103[.]35[.]191[.]137

AS44477

2024-06-12

2025-05-04

lexisnex[.]team

103[.]35[.]191[.]137

AS44477

2024-06-11

2025-05-05

lexisnex[.]top

103[.]35[.]191[.]137

AS44477

2024-06-11

2025-05-03

lexisnexis[.]day

89[.]105[.]198[.]190

AS204601

2024-05-01

2025-05-01

lexisnexis[.]lat

103[.]35[.]190[.]40

AS44477

2024-06-14

2025-03-30

lexisnexis[.]one

103[.]35[.]191[.]137

AS44477

2024-06-05

2025-05-04

lexisnexis[.]pro

103[.]35[.]191[.]137

AS44477

2024-05-07

2025-05-05

lexisnexis[.]top

103[.]35[.]191[.]137

AS44477

2024-06-07

2025-05-04

meet-go[.]info

103[.]113[.]70[.]158

AS44477

2024-05-07

2025-05-02

meet[.]com[.]de

45[.]89[.]53[.]243

AS44477

2024-05-23

2025-02-16

sapconcur[.]top

86[.]104[.]72[.]208

AS44477

2024-06-13

2025-05-04

thomsonreuter[.]info

86[.]104[.]72[.]16

AS44477

2024-06-15

2025-05-04

thomsonreuter[.]pro

86[.]104[.]72[.]16

AS44477

2024-06-15

2025-05-05

wsj[.]pm

103[.]113[.]70[.]37

AS44477

2024-04-19

2025-04-19

Table 1: *Domains linked to Infection Vector 1 still resolving as of 2025 (Source: Recorded Future)*

Fake update websites often use the same script designed to fingerprint the host system, consisting of the functions getIPAddress() and trackPageOpen(). As previously reported, these scripts usually send a POST request to a CDN-themed domain, such as *cdn40[.]click* (see **Figure 2**). These domains typically begin with "cdn" followed by a random number and a top-level domain (TLD). The malicious payload is commonly delivered via the /download.php endpoint. However, Insikt Group has also identified variations, including /download/download.php, download2.php, and product-specific paths (such as /download/aimp_5.30.2541_w64-release.exe). Additionally, in at least one case, the threat actors appeared to use a compromised domain — *worshipjapan[.]com* — for fingerprinting purposes. This activity was observed on a website associated with the domain *as4na[.]com*.

Figure 2: *Typical JavaScript functions found on fake update pages such as meet-go[.]click (Source: URLScan)*

Notably, while most domains associated with Infection Vector 1 are crafted to impersonate legitimate software products, some appear to be randomly generated or arbitrary. Examples include *testsstestststests003202[.]shop*, which is tied to the email address *kasalboov@web[.]de*, according to its WHOIS record. This same email is also linked to domains such as *lexisnexis[.]pro*, *aimp[.]xyz*, *concur[.]life*, *cdn3535[.]shop*, and *cdn251[.]lol*. Additional anomalies include domains like *gogogononono[.]top* and *gogogononono[.]xyz*, both hosted on the IP address *103[.]35[.]190[.]40*, which also hosts lexisnexis[.]lat.

Although the first Advanced IP Scanner–themed domains linked to GrayAlpha, as discussed in this report, began resolving in early 2024 (see **Figure 3**), Insikt Group had already observed FIN7 leveraging a fake Advanced IP Scanner domain to compromise victims as early as the second half of 2023. Specifically, during a brief period at the end of September 2023, Insikt Group identified over 212 infected systems communicating with a FIN7-controlled Carbanak C2 server *166[.]1[.]160[.]118* via TCP port 443. While this activity was initially attributed to the exploitation of a one-day vulnerability chain, subsequent analysis revealed that the infections were instead linked to the typosquatted domain *advanced-ip-sccanner[.]com* — which was hosted behind Cloudflare at the time.

Figure 3: *Fake Advanced IP Scanner download page on advancedipscannerapp[.]com (Source: URLScan)*

Hosting Analysis

The vast majority of domains associated with Infection Vector 1 resolved to infrastructure operated by the bulletproof hoster, Stark Industries Solutions (AS44477), with additional hosting observed on AS29802 (HIVELOCITY, Inc.) and AS41745 (FORTIS-AS) (see **Figure 4**). Notably, infrastructure within AS29802 consisted of IP space controlled by bulletproof hoster 3NT Solutions LLP and announced via HIVELOCITY. Hosting infrastructure for Infection Vector 2 is predominantly concentrated within AS41745, as detailed further in the **Infection Vector 2: 7-Zip Impersonation** section of this report.

Figure 4: Breakdown of ASNs as observed with Infection Vector 1 (Source: Recorded Future)

FORTIS-AS (AS41745), commonly referenced by its responsible organization, “Baykov Ilya Sergeevich” (ORG-HIP1-RIPE), has been repeatedly leveraged in activities related to FIN7. In addition to infrastructure linked to Stark Industries Solutions, FORTIS-AS has hosted infrastructure used to deploy malware families such as POWERTRASH and DiceLoader, both of which are directly associated with FIN7 operations.

According to the WHOIS record for netblock *85[.]209[.]134[.]0/24*, which is used by GrayAlpha, the block is assigned to Baykov Ilya Sergeevich (ORG-HIP1-RIPE). This entity is closely tied to the infrastructure service provider (ISP) “hip-hosting”, with multiple contact points and technical references — including domains such as *fortis[.]host* and *hip-hosting[.]com* — appearing throughout the record (see **Figure 5**).

Figure 5: *Contact details linked to Baykov Ilya Sergeevich (Source: Recorded Future)*

Insikt Group assesses with high confidence that “hip-hosting” is the ISP behind the entity “Baykov Ilya Sergeevich” (ORG-HIP1-RIPE). This assessment is supported by multiple corroborating data points in the WHOIS record and RIPE ORG object for ORG-HIP1-RIPE.

To read the entire analysis, click here to download the report as a PDF.