CYBER
THREAT
ANALYSIS

Recorded Future®

Insikt Group®

February 18, 2026

GrayCharlie Hijacks Law Firm Sites in Suspected Supply-Chain Attack

GrayCharlie, overlapping with SmartApeSG, injects JavaScript into hacked WordPress sites, redirecting users to fake update pages or ClickFix pop-ups delivering NetSupport RAT, Stealc, and SectopRAT.

Insikt Group identified extensive infrastructure, including C2 servers, staging infrastructure spanning actor-controlled and compromised hosts, and components of higher-tier infrastructure.

Insikt Group analyzed two GrayCharlie attack chains: fake browser-update pages reached via compromised sites, and ClickFix pop-ups, a technique that became increasingly common in 2025.

Analysis cut-off date: December 9, 2025

Executive Summary

Insikt Group has been monitoring GrayCharlie, a threat actor overlapping with SmartApeSG[1] and active since mid-2023, for some time, and is now publishing its first report on the group. GrayCharlie compromises WordPress sites and injects them with links to externally hosted JavaScript that redirects visitors to NetSupport RAT payloads delivered via fake browser update pages or ClickFix mechanisms. These infections often progress to the deployment of Stealc and SectopRAT. Insikt Group identified a large amount of infrastructure linked to GrayCharlie, primarily tied to MivoCloud and HZ Hosting Ltd. This includes NetSupport RAT command-and-control (C2) servers, both actor-controlled and compromised staging infrastructure, and higher-tier infrastructure used to administer operations. While most compromised websites appear to be opportunistic and span numerous industries, Insikt Group identified a cluster of United States (US) law firm sites that were likely compromised around November 2025, possibly through a supply-chain compromise involving a shared IT provider.

To protect against GrayCharlie, security defenders should block IP addresses and domains tied to associated remote access trojans (RATs) and infostealers, flag and potentially block connections to compromised websites, and deploy updated detection rules (YARA, Snort, Sigma) for current and historical infections. Other controls include implementing email filtering and data exfiltration monitoring. See the **Mitigations** section of this report for implementation guidance and **Appendix A** for a complete list of indicators of compromise (IoCs).

Key Findings

- GrayCharlie, which overlaps with SmartApeSG and first emerged in mid-2023, is a threat actor that injects links to externally hosted JavaScript into compromised WordPress sites. These links redirect victims to NetSupport RAT infections delivered via fake browser update pages or ClickFix techniques, ultimately resulting in Stealc and SectopRAT infections.
- Insikt Group identified a wide range of GrayCharlie infrastructure, largely associated with MivoCloud and HZ Hosting Ltd. This includes NetSupport RAT command-and-control (C2) servers, staging infrastructure made up of both actor-controlled and compromised infrastructure, as well as components of GrayCharlie's higher-tier infrastructure used to manage its operations.
- Insikt Group identified two primary attack chains associated with GrayCharlie: one in which victims encounter fake browser update pages after visiting compromised websites, and another in which they are presented with a ClickFix pop-up, a technique that has become increasingly common in 2025.

[1] SmartApeSG can refer to either a malware campaign or a threat group.

Background

GrayCharlie is Insikt Group's designation for a threat activity group that first appeared in mid-2023 and is behind SmartApeSG, also referred to as ZPHP or HANEYMANEY. The group's operations typically involve injecting malicious JavaScript into legitimate but compromised WordPress sites. Visitors to these sites are shown convincing, browser-specific fake update prompts (such as for Chrome, Edge, or Firefox) that encourage them to download what appears to be an update but is actually malware.

In late March or early April 2025, SmartApeSG shifted from using fake browser updates to deploying ClickFix lures, mirroring a broader trend among threat actors of increasingly adopting ClickFix.

GrayCharlie predominantly delivers NetSupport RAT; however, deployments of Stealc and, more recently, SectopRAT, have been observed in rare instances. The group's ultimate objectives remain uncertain. Current evidence suggests a focus on data theft and financial gain, with a theoretical, but unsubstantiated, possibility that it may sell or transfer access to other threat actors.

Threat Analysis

Insikt Group has been tracking GrayCharlie for an extended period and has observed the actor's persistent behavior since its emergence in 2023. GrayCharlie continues to conduct the same types of operations, regularly deploying large volumes of new infrastructure and adhering to consistent tactics, techniques, and procedures (TTPs), including continued use of the same infection chains and NetSupport RAT payloads. The group targets organizations worldwide, with a particular focus on the US. The following sections provide a detailed examination of GrayCharlie's operational infrastructure and its two primary attack chains.

Infrastructure Analysis

NetSupport RAT Clusters

Insikt Group identified two main NetSupport RAT clusters linked to GrayCharlie based on factors such as TLS certificates, NetSupport serial numbers and license keys, and the timing of the activity (see **Figure 1**). In addition, Insikt Group identified a range of other NetSupport RAT C2 servers linked to GrayCharlie activity, but which are not currently attributed to either of the two main clusters. Insikt Group assesses that these clusters may correspond either to different individuals associated with GrayCharlie or to distinct GrayCharlie campaigns. The clusters are further described below.

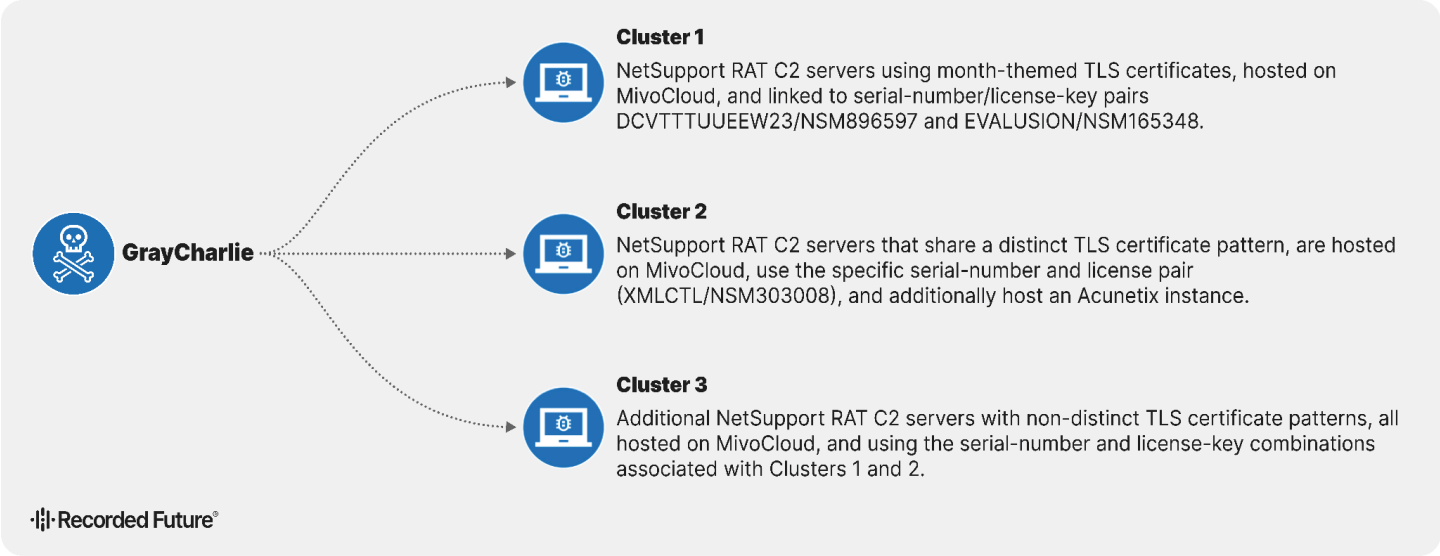

Figure 1: *Overview of GrayCharlie clusters observed in 2025 (Source: Recorded Future)*

Cluster 1

Cluster 1 comprises NetSupport RAT C2 servers whose TLS certificates display a recurring monthly naming pattern. All servers in this cluster are hosted by MivoCloud and were deployed between March and August 2025. Notably, NetSupport RAT samples associated with the cluster's March and April infrastructure used the license key `DCVTTTUUEEW23` and serial number `NSM896597`, before shifting to the license key `EVALUSION` and serial number `NSM165348` in subsequent deployments. The C2 servers associated with this cluster are listed in **Table 1**.

IP Address	TLS Common Name	License Key	Serial Number
194[.]180[.]191[.]51	mar5	DCVTTTUUEEW23	NSM896597
194[.]180[.]191[.]168	mar4	DCVTTTUUEEW23	NSM896597
194[.]180[.]191[.]171	mar3	DCVTTTUUEEW23	NSM896597
5[.]181[.]159[.]60	mar1	DCVTTTUUEEW23	NSM896597
194[.]180[.]191[.]17	mar2	DCVTTTUUEEW23	NSM896597
94[.]158[.]245[.]66	apr2	DCVTTTUUEEW23	NSM896597
94[.]158[.]245[.]81	apr3	DCVTTTUUEEW23	NSM896597
185[.]225[.]17[.]74	apr4	DCVTTTUUEEW23	NSM896597
194[.]180[.]191[.]189	apr1	DCVTTTUUEEW23	NSM896597

IP Address	TLS Common Name	License Key	Serial Number
5[.]252[.]178[.]123	may5	EVALUSION	NSM165348
94[.]158[.]245[.]104	may1	EVALUSION	NSM165348
94[.]158[.]245[.]115	may2	EVALUSION	NSM165348
94[.]158[.]245[.]118	may3	EVALUSION	NSM165348
94[.]158[.]245[.]131	may4	EVALUSION	NSM165348
94[.]158[.]245[.]137	may53	EVALUSION	NSM165348
94[.]158[.]245[.]13	june2	EVALUSION	NSM165348
94[.]158[.]245[.]174	june6	EVALUSION	NSM165348
94[.]158[.]245[.]140	june1	EVALUSION	NSM165348
185[.]163[.]45[.]30	june7	EVALUSION	NSM165348
94[.]158[.]245[.]63	june3	EVALUSION	NSM165348
94[.]158[.]245[.]111	june7	EVALUSION	NSM165348
94[.]158[.]245[.]135	june5ebatquot	EVALUSION	NSM165348
5[.]252[.]178[.]23	july9	EVALUSION	NSM165348
185[.]163[.]45[.]41	july1	EVALUSION	NSM165348
185[.]163[.]45[.]61	july3	EVALUSION	NSM165348
185[.]163[.]45[.]73	july4	EVALUSION	NSM165348
185[.]163[.]45[.]87	july6	EVALUSION	NSM165348
185[.]163[.]45[.]97	july8	EVALUSION	NSM165348
185[.]163[.]45[.]130	july9	EVALUSION	NSM165348

Table 1: *NetSupport RAT C2 servers linked to Cluster 1 (Source: Recorded Future)*

Notably, the NetSupport RAT C2 servers in Cluster 1 are connected not only through the characteristics previously described, but also by the near-simultaneous creation of their TLS certificates. For example, the TLS certificate with the common name `june5ebatquot` associated with IP address *94[.]158[.]245[.]135* was generated on June 30, 2025 at 4:55:20 PM, while the certificate with the common name june6 linked to *94[.]158[.]245[.]174* was created only 20 seconds later.

Cluster 2

Cluster 2 comprises NetSupport RAT command-and-control servers whose TLS certificates typically start with two or more repetitions of "s", followed by an "i" and a number (so "`sssi3`", for example). NetSupport RAT samples linked to Cluster 2 used the license key `XMLCTL` and serial number `NSM303008`. The NetSupport RAT C2 servers typically also host an instance of the vulnerability scanner Acunetix. The C2 servers associated with this cluster are listed in **Table 2**. Notably, all TLS certificates associated with this cluster were created in a single batch on June 17, 2025.

IP Address	TLS Common Name	License Key	Serial Number
5[.]181[.]159[.]112	sssi3	XMLCTL	NSM303008
5[.]181[.]159[.]9	ssi1	XMLCTL	NSM303008
5[.]181[.]159[.]38	sssi2	XMLCTL	NSM303008
5[.]181[.]159[.]140	ssssi6	XMLCTL	NSM303008
5[.]181[.]159[.]143	ssssi8	XMLCTL	NSM303008
5[.]181[.]159[.]142	sssssi7	XMLCTL	NSM303008
5[.]181[.]159[.]139	ssssi5	XMLCTL	NSM303008

Table 2: *NetSupport RAT C2 servers linked to Cluster 2 (Source: Recorded Future)*

Of note, one NetSupport RAT C2 server (*94[.]158[.]245[.]56*) used a TLS certificate with the common name 23sss, created in May 2025, and was linked to a NetSupport RAT sample that carried the same license key (`EVALUSION`) and serial number (`NSM165348`) previously observed in Cluster 1.

Other NetSupport RAT C2 Servers

Insikt Group identified an additional set of NetSupport RAT C2 servers linked to GrayCharlie that did not form a distinct cluster (see **Table 3**). However, all the servers were hosted by MivoCloud and were associated with NetSupport RAT samples using license key and serial number combinations observed in Clusters 1 and 2.

IP Address	TLS Common Name	License Key	Serial Number
5[.]181[.]159[.]29	ssdecservicsdes	N/A	N/A
194[.]180[.]191[.]18	papichssd2	DCVTTTUUEEW2	NSM896597
94[.]158[.]245[.]153	kosmo2	XMLCTL	NSM303008
94[.]158[.]245[.]170	normvork	XMLCTL	NSM303008
5[.]181[.]159[.]62	ffdds	DCVTTTUUEEW23	NSM896597
5[.]181[.]156[.]234	wedn1	XMLCTL	NSM303008
5[.]252[.]178[.]35	scgs234123	XMLCTL	NSM303008
194[.]180[.]191[.]209	novemsdf	XMLCTL	NSM303008
5[.]181[.]156[.]244	wends4	XMLCTL	NSM303008
194[.]180[.]191[.]121	novaksuur	EVALUSION	NSM165348
5[.]252[.]177[.]120	lohsd	XMLCTL	NSM303008
5[.]252[.]177[.]15	bounce	XMLCTL	NSM303008
185[.]163[.]45[.]16	update1	XMLCTL	NSM303008

Table 3: *Additional NetSupport RAT C2 servers linked to GrayBravo (Source: Recorded Future)*

Staging Infrastructure

Once GrayCharlie victims land on the compromised WordPress sites, thereby satisfying the conditional logic, the payload is typically fetched from the attacker-controlled infrastructure and injected into the compromised WordPress sites. Insikt Group has identified two distinct types of staging infrastructure, each characterized by different website templates. Type 1 is modeled after "Wiser University," and Type 2 is modeled after "Activitar."

Type 1: "Wiser University"

The IP addresses associated with the Type 1 staging infrastructure are linked to websites impersonating "Wiser University" (see **Figure 2**), a fictional entity used to demonstrate Wiser, a free Bootstrap HTML5 education website template for school, college, and university websites. (As a sidenote, Oreshnik is the name of a Russian intermediate-range ballistic missile reportedly capable of speeds exceeding Mach 10.) **Appendix B** lists the IP addresses associated with the Type 1 staging infrastructure. All IP addresses, except for one, are announced by AS202015 (HZ Hosting Ltd).

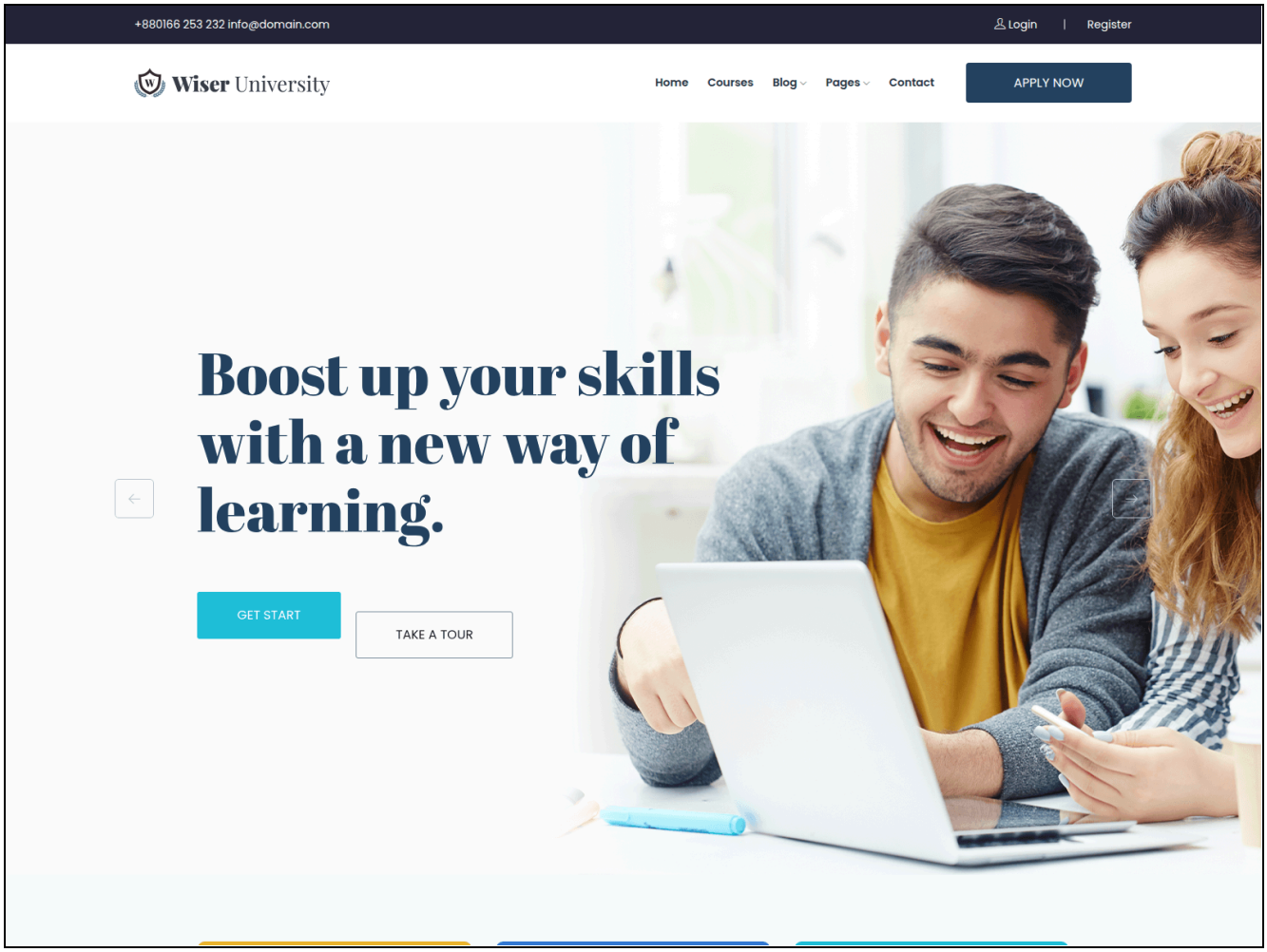

Figure 2: *Website impersonating "Wiser University" (Source: Recorded Future)*

Suspected Testing Infrastructure

Although most IP addresses associated with the Type 1 staging infrastructure are announced by AS202015, as shown in **Appendix B**, Insikt Group also identified a small subset announced by other ASNs that host the same websites (see **Table 4**). On average, approximately one such IP address appears to be established each month. Notably, most of these IP addresses appear to geolocate to Russia, and the same ASNs are consistently reused within the same timeframe.

IP Address	ASN	Country	Date of Emergence
89[.]253[.]222[.]25	AS41535	RU	2025-08-29
89[.]253[.]222[.]156	AS41535	RU	2025-08-26
89[.]169[.]12[.]48	AS207957	GB	2025-07-08
185[.]231[.]245[.]158	AS202984	RU	2025-06-27
95[.]182[.]123[.]86	AS202984	RU	2025-05-19
23[.]140[.]40[.]66	AS61400	RU	2025-04-11
217[.]114[.]15[.]253	AS198610	RU	2025-04-09
45[.]153[.]191[.]245	AS198610	RU	2025-03-21
46[.]29[.]163[.]28	AS51659	RU	2025-02-06

Table 4: *Additional infrastructure possibly linked to GrayCharlie (Source: Recorded Future)*

Type 2: "Activitar"

Insikt Group identified an additional set of staging infrastructure, referred to as "Type 2." The IP addresses in this cluster commonly host specific websites (see **Figure 3**). Insikt Group assesses that this template was sourced elsewhere and is not unique to GrayCharlie.

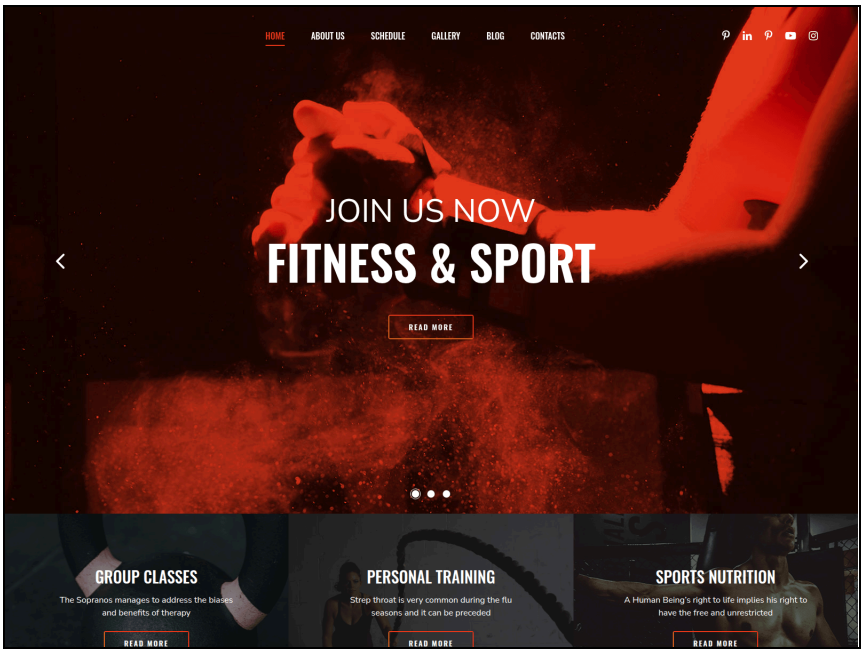

Figure 3: *Website impersonating "Activitar" (Source: Recorded Future)*

A subset of domains and IP addresses associated with Type 2 is presented in **Table 5**. Notably, most of the IP addresses are also announced by AS202015 (HZ Hosting Ltd), and one domain in **Table 5**, *filmlerzltyazilimsx[.]shop*, is linked to the email address *oreshnik[@]mailum[.]com* through its WHOIS record.

Domain	IP Address	ASN
filmlerzltyazilimsx[.]shop	79[.]141[.]163[.]169	AS202015
foolowme[.]com	144[.]172[.]115[.]211	AS14956
joiner[.]best	79[.]141[.]162[.]135	AS202015
lowi1[.]com	185[.]33[.]86[.]11	AS202015
morniksell[.]com	172[.]86[.]90[.]84	AS14956
persistancejs[.]store	185[.]80[.]53[.]79	AS59711
pomofight[.]com	45[.]61[.]134[.]76	AS14956
port4loms[.]com	194[.]15[.]216[.]118	AS197155
signaturepl[.]com	77[.]83[.]199[.]162	AS202015
yungask[.]com	91[.]193[.]19[.]220	AS202015

Table 5: *Domains and IP addresses linked to Type 2 staging infrastructure (Source: Recorded Future)*

Compromised Infrastructure

GrayCharlie commonly injects malicious scripts into the Document Object Model (DOM) of compromised WordPress sites using script tags. Insikt Group has identified several recurring URL patterns tied to this activity: some URLs load externally hosted JavaScript files (such as *hxxps://joiner[.]best/work/original[.]js*), while others call a PHP file on specific endpoints using an ID parameter (such as *hxxps://signaturepl[.]com/work/index[.]php?abje2LAw*). Notably, these URLs are updated over time by the threat actor, complicating detection and indicating the threat actor maintains ongoing access to a large pool of compromised WordPress installations. **Appendix A** lists a subset of WordPress websites infected by GrayCharlie.

Although the exact initial access vector is unknown, it is likely that the actors either purchase access, such as via malware logs containing WordPress admin credentials, or exploit vulnerable WordPress plugins. The latter remains the most frequent cause of all WordPress compromises.

Suspected Compromise of "Law Firm Acceleration Company" SMB Team

While the GrayCharlie-linked compromised WordPress sites span a wide range of industry verticals, in a few rare instances, the threat actors appear to have obtained, either through their own intrusions or via a third party, a more targeted set of WordPress domains. Specifically, at least fifteen websites belonging to US law firms were observed loading the external JavaScript hosted at *hxxps://persistancejs[.]store/work/original[.]js* (see **Table 6**).

Insikt Group assesses that GrayCharlie (or the third party GrayCharlie works with) likely compromised these websites through a supply-chain vector. One potential avenue is SMB Team, the self-described "fastest-growing law firm acceleration company," which has supported thousands of firms across North America, according to its website, as its logo and other references appear across many of the websites listed in **Table 6** (see **Figure 4**). Notably, credentials associated with an SMB Team email address used for a WordPress hosting platform surfaced around the same time that the domain *persistancejs[.]store* first began resolving. This temporal overlap suggests that the threat actors may have gained access to SMB Team-related infrastructure through the use of legitimate, compromised credentials.

Domain	Company	Country	SMB Team
bianchilawgroup[.]com	Bianchi Law Group	US	Yes
brattonlawgroup[.]com	Bratton Law Group	US	Yes
brighterdaylaw[.]com	Brighter Day Law	US	N/A
defensegroup[.]com	The Defense Group	US	Yes
dwicriminallawcenter[.]com	Benjamin Law Firm LLC	US	Yes
fisherstonelaw[.]com	Fisher Stone, P.C.	US	Yes
jarrettfirm[.]com	Jarrett & Price LLC	US	Yes
raineyandrainey[.]com	Rainey & Rainey Attorneys At Law PLLC	US	Yes
rbbfirm[.]com	Buchanan Law Group	US	Yes
rmvlawyer[.]com	The Law Office of Brian Simoneau, P.C.	US	Yes
www[.]brentadams[.]com	Brent Adams & Associates	US	Yes
www[.]cfblaw[.]com	Cohen Forman Barone, PC	US	Yes
www[.]gerlinglaw[.]com	Gerling Law Injury Attorneys	US	Yes
www[.]immigration-defense[.]com	Law Offices of Daniel Shanfield	US	Yes

Domain	Company	Country	SMB Team
www[.]schwartzandschwartz[.]com	Schwartz & Schwartz Attorneys at Law, P.A.	US	N/A

Table 6: *Compromised law firm websites linked to GrayCharlie (Source: Recorded Future)*

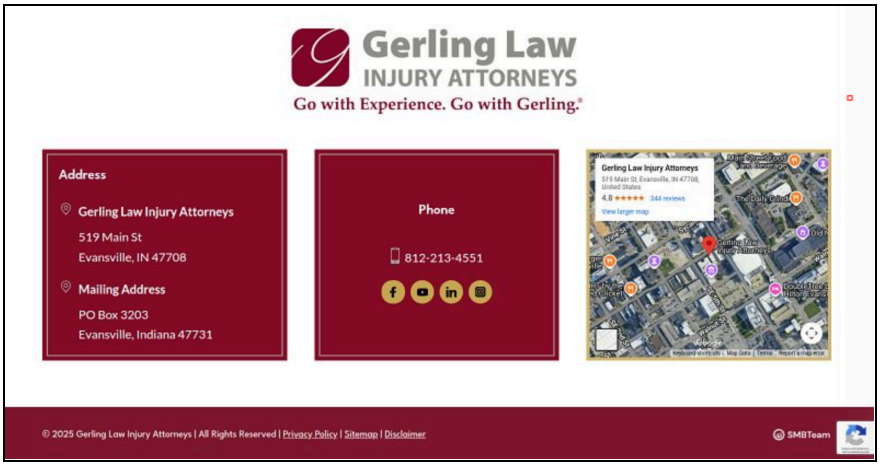

Figure 4: *Website of Gerling Law Injury Attorneys (left) and SMBTeam logo (right) (Source: URLScan)*

Notably, while an SMB Team compromise is possible, Insikt Group also assesses that the actors may have exploited a specific version of WordPress or its plugins used by SMB Team, which could explain the simultaneous compromise of all affected websites.

In some instances, the same compromised WordPress sites are compromised by multiple threat actors simultaneously. For example, *bianchilawgroup[.]com* was also breached by TAG-124 (also known as LandUpdate808 or Kongtuke) since at least December 2025, which used the domain *vimsltd[.]com*.

Higher-Tier Analysis

GrayCharlie administers its staging infrastructure primarily over SSH, though other ports are used intermittently. The group manages its NetSupport RAT C2 servers over TCP port 443. Overall, Insikt Group assesses that GrayCharlie relies extensively on proxy services to administer its infrastructure. Additionally, based on presumed browsing activity from higher-tier servers, at least some individuals linked to GrayCharlie are assessed to be Russian-speaking.

Attack-Chain Analysis

GrayCharlie has been observed using two different attack chains to deliver NetSupport RAT. The first chain uses compromised websites to distribute a fake browser update that triggers the retrieval and installation of a script-based payload; the second chain uses compromised WordPress sites and a ClickFix-style lure that copies a command to fetch and install the RAT. Both culminate in NetSupport execution from `%AppData%`, Registry Run key persistence, and C2 connectivity; the technical details are expanded below.

Attack Chain 1: Fake Browser Update Leading to NetSupport RAT

According to public reporting, when GrayCharlie first became active in mid-2023, it relied on fake browser updates to deliver the NetSupport RAT. Although the group later shifted to the ClickFix technique, Insikt Group observed a return to fake browser updates as early as October 12, 2025. **Figure 5** provides an overview of Attack Chain 1.

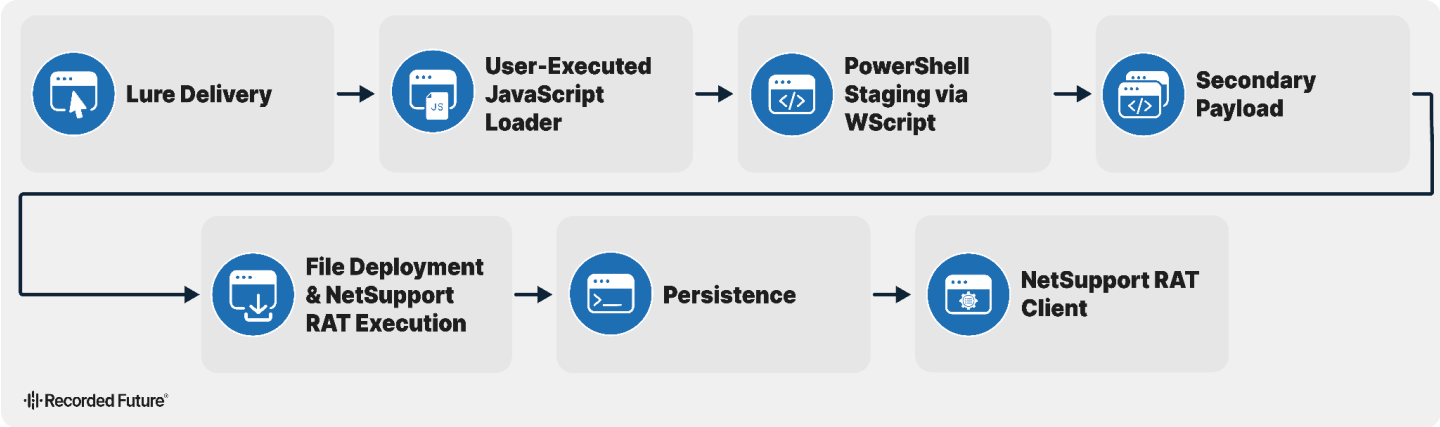

Figure 5: *Attack Chain 1 (Source: Recorded Future)*

1. **Website compromise and lure delivery**. Threat actors modify legitimate sites to load malicious scripts that render a browser-specific "update" prompt. Selecting the prompt initiates download of a ZIP "update" package containing a primary JavaScript file alongside decoy `.dat` files.
2. **User-executed JavaScript loader**. The victim manually runs the `.js` script. The script mimics a benign browser component to reduce suspicion while silently initiating the next stage of the attack.
3. **PowerShell staging via WScript**. The JavaScript launches `wscript.exe`, which spawns `powershell.exe`. PowerShell reaches out to a remote host to fetch an obfuscated JavaScript containing encoded tasking.
4. **Secondary payload retrieval**. PowerShell decodes instructions and downloads the actual payload ZIP archive. This archive contains a complete NetSupport RAT client set, including `client32.exe` and required DLLs.

5. **File deployment and execution**. The archive is extracted under the user profile (for example, `%AppData%\Roaming\...`). `client32.exe` is started in the background to minimize visible indicators to the user.
6. **Persistence establishment**. A Windows Run registry key is created to automatically launch `client32.exe` at logon, ensuring the NetSupport RAT remains active after reboots without requiring further user interaction.
7. **C2 readiness**. With the NetSupport RAT client running on the infected host, the endpoint is prepared to establish command-and-control connectivity with the attacker's infrastructure.

Attack Chain 2: WordPress Redirects and ClickFix Leading to NetSupport RAT

As early as April 2025, GrayCharlie began using ClickFix as a secondary attack chain, consistent with industry reporting that many threat actors have adopted ClickFix techniques due to their effectiveness. **Figure 6** provides an overview of Attack Chain 2.

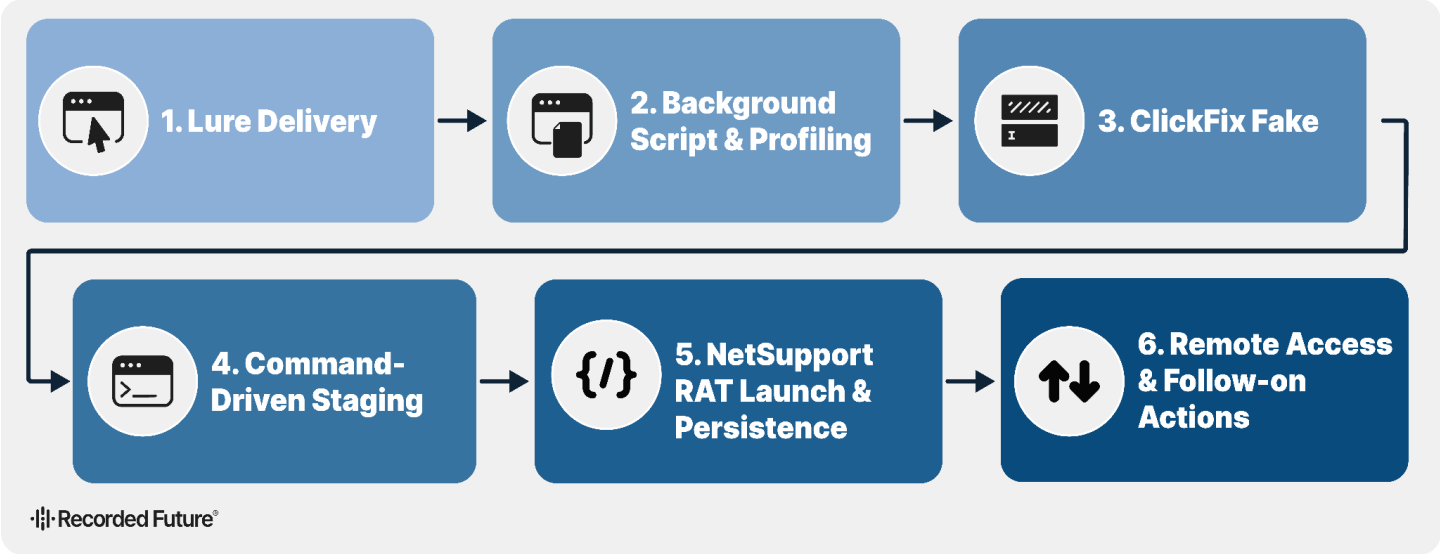

Figure 6: *Attack Chain 2 (Source: Recorded Future)*

1. **Initial delivery and redirection.** Phishing emails, malicious PDFs, or links on gaming sites direct users to compromised WordPress pages that embed attacker JavaScript.
2. **Background script and profiling.** A background script loads when the site is visited, injects an iframe, and profiles the environment (such as the operating system and browser) to deliver the next stage.
3. **ClickFix fake CAPTCHA.** The page presents a fake CAPTCHA that quietly copies a malicious command to the user's clipboard and instructs them to paste it into the Windows Run dialog (Win+R), turning social engineering into user-assisted execution (see **Figure 7**).

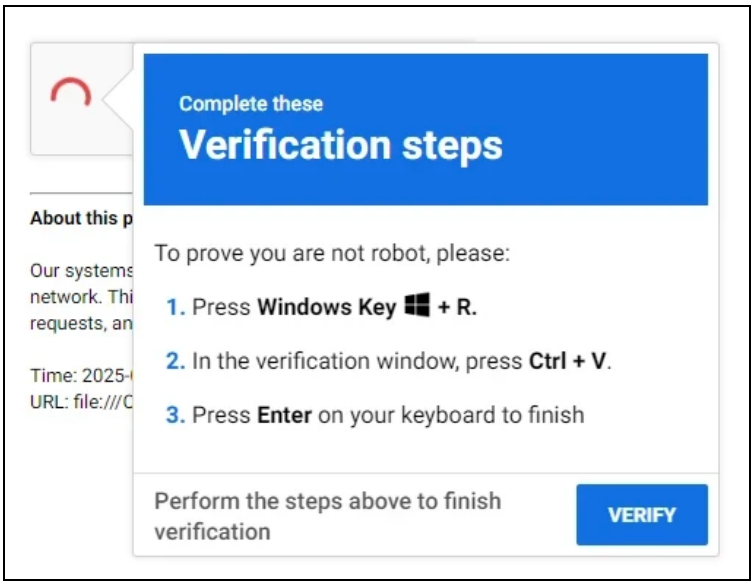

Figure 7: *Fake Captcha (Source: Elastic)*

4. **Command-driven staging.** The pasted command retrieves a batch file that downloads a ZIP containing NetSupport RAT and uses PowerShell to extract it into `%AppData%\Roaming\` (see **Figure 8**).

```
powershell -Win^dow Style Hidden -Command "Add-Type -AssemblyName 'System.
IO.Compression FileSystem';
[IO.Compression.ZipFile]::ExtractToDirectory('!CF0JOAXML!','!WFHEYHKMZ!')"
```

Figure 8: *PowerShell command (Source: Cybereason)*

5. **NetSupport RAT launch and persistence.** The batch file starts `client32.exe` and sets a Run registry key to automatically relaunch the NetSupport RAT client at startup, establishing persistence on the endpoint.
6. **Remote access and follow-on actions.** Once connected to C2, operators can interact with the system, perform reconnaissance (for example, domain group membership queries), transfer files, execute additional commands, and potentially move laterally using access acquired from the host.

Observed Operator Activity

In October 2025, Insikt Group detonated a NetSupport RAT sample (SHA256: 31804c48f9294c9fa7c165c89e487bfbebeda6daf3244ad30b93122bf933c79c) with the C2 server *5[.]181[.]156[.]234[:]443* linked to GrayCharlie within a controlled environment. Later that day, approximately three hours later, the threat actor connected using NetSupport RAT, compressed and moved two files, and then executed group and account reconnaissance commands. The same actor

returned three days later and repeated the previously observed reconnaissance commands (see **Figure 9**).

```
net group /domain "Domain COmputers"
C:\Windows\system32\net1 group /domain "Domain COmputers"
```

Figure 9: *Reconnaissance commands (Source: Recorded Future)*

When both files were compressed into a single ZIP archive and the executable was detonated, the process sideloaded a DLL identified as Sectop RAT (SHA256: 59e7e7698d77531bfbfea4739d29c14e188b5d3109f63881b9bcc87c72e9de78) with the C2 server *85[.]158[.]110[.]179[:]15847*. The executable (SHA256: 5f1bd92ad6edea67762c7101cb810dc28fd861f7b8c62e6459226b7ea54e1428) was identified as "Merge XML Files", version 1.2.0.0, developed by Vovsoft, and was signed with a digital certificate that expired on October 31, 2025.

Mitigations

- Leverage the IoCs in **Appendix A** and **Appendix B** to investigate potential past or ongoing infections, both successful and attempted; Recorded Future customers can use the Recorded Future Intelligence Operations Platform to monitor for future IoCs associated with GrayCharlie.
- Monitor for validated infrastructure associated with the malware families discussed in this report, including NetSupport RAT and Stealc, as well as numerous others identified and validated by Insikt Group, and integrate these indicators into relevant detection and monitoring systems.
- Leverage the Sigma, YARA, and Snort rules provided in **Appendices D**, **E**, and **F** in your security information and event management (SIEM) or endpoint detection and response (EDR) tools to detect the presence or execution of NetSupport RAT. Customers can use additional detection rules available in the Recorded Future Intelligence Operations Platform.
- Use Recorded Future Network Intelligence to detect instances of data exfiltration from your corporate infrastructure to known malicious infrastructure.
- Use the Recorded Future Intelligence Operations Platform to monitor GrayCharlie, other threat actors, and the broader cybercriminal ecosystem, ensuring visibility into the latest tactics, techniques, and procedures (TTPs), preferred tools and services (for example, specific threat activity enablers [TAEs] used by threat actors), and emerging developments.
- Use Recorded Future AI's reporting feature to generate tailored reports on topics that matter to your company. For example, if you want to stay informed about activities related to GrayCharlie, you can receive regular AI-generated updates on this threat actor.

Outlook

GrayCharlie has been operating for more than two years, and despite shifts in its tactics, such as alternating between fake updates and ClickFix techniques or transitioning from SmartApe to other hosting providers like MivoCloud, the group's core behaviors have remained consistent. Given its sustained activity, GrayCharlie is highly likely to remain active and continue targeting organizations worldwide, with a current emphasis on US entities, as indicated by Recorded Future Network Intelligence.

Insikt Group will continue to closely monitor GrayCharlie to detect emerging threats and evaluate the group's strategic direction within the broader cybercriminal ecosystem.

Appendix A: Indicators of Compromise

Cluster 1 NetSupport RAT C2 IP Addresses:

5[.]181[.]159[.]60
5[.]252[.]178[.]23
5[.]252[.]178[.]123
94[.]158[.]245[.]13
94[.]158[.]245[.]63
94[.]158[.]245[.]66
94[.]158[.]245[.]81
94[.]158[.]245[.]104
94[.]158[.]245[.]111
94[.]158[.]245[.]115
94[.]158[.]245[.]118
94[.]158[.]245[.]131
94[.]158[.]245[.]135
94[.]158[.]245[.]137
94[.]158[.]245[.]140
94[.]158[.]245[.]174
185[.]163[.]45[.]30
185[.]163[.]45[.]41
185[.]163[.]45[.]61
185[.]163[.]45[.]73
185[.]163[.]45[.]87
185[.]163[.]45[.]97
185[.]163[.]45[.]130
185[.]225[.]17[.]74
194[.]180[.]191[.]17
194[.]180[.]191[.]51
194[.]180[.]191[.]168
194[.]180[.]191[.]171
194[.]180[.]191[.]189

Cluster 2 NetSupport RAT C2 IP Addresses:

5[.]181[.]159[.]9
5[.]181[.]159[.]38
5[.]181[.]159[.]112
5[.]181[.]159[.]139
5[.]181[.]159[.]140
5[.]181[.]159[.]142
5[.]181[.]159[.]143

Other NetSupport RAT C2 Servers:

5[.]181[.]156[.]234
5[.]181[.]156[.]244
5[.]181[.]159[.]29
5[.]181[.]159[.]62
5[.]252[.]177[.]15
5[.]252[.]177[.]120
5[.]252[.]178[.]35
94[.]158[.]245[.]153

94[.]158[.]245[.]170
185[.]163[.]45[.]16
194[.]180[.]191[.]18
194[.]180[.]191[.]121
194[.]180[.]191[.]209

NetSupport RAT Hashes:
06a0a243811e9c4738a9d413597659ca8d07b00f640b74adc9cb351c179b3268
0e9df9294c36702eee970efcb4a70b6ddb433190ab661273e2e559185c55b6c1
112bf17e7c0d0695e9229d60f0d2734c6b96d7edfb41ea3e98e518f4fb1ae6e9
11370e108c8e7a53e52f01df0829c8addb5833145618a7701fbedbb1d837a43d
15dfe9d443027ba01b8f54f415fd74d373b3a06017db8ef110fb55b33357b190
16c8b5e10135d168d73a553a4bda51628e5b4fd419c0ecd47ca4cd7aa864ebd5
18df68d1581c11130c139fa52abb74dfd098a9af698a250645d6a4a65efcbf2d
1900ca9b482273df3127e221526023c025808d8fd65769a418fe1f346e7d41e2
1c389bf1859a00c58b6a97c02fc26c2fe9766c43e06242a94e92b6585b62398b
21a24922b29742977c4f7e25dd2be056dc02bc5e70c98e32ec3e0c6206f4d9ef
312a0e4db34a40cb95ba1fac8bf87deb45d0c5f048d38ac65eb060273b07df67
31804c48f9294c9fa7c165c89e487bfbebeda6daf3244ad30b93122bf933c79c
31f69d67eca6f3fc837e8d10dff4e2fb6643e33c118cff87df4fee2b183bf0e0
37e8b57ff4d724053b1917dc6edaca0708d44ceecd00cab7e4cabb336c2868d7
3ac57bea954ce68dc937f6954ae8a6a19a367a579aeeda7cc93ddd5968fae250
3ada20fbd80ec7f536db8303a5fa029af741a6914de61376ac8f81ac3ac728fd
3b5658532bc4058131689c5641def85d7ae25d5b837d3d1aff3af7bb25581f17
3c499faac4b973c237670f046973691a245ecd735ffebcca3e93337d94b71cde
3c4b87be8450e3120b7ad2b11ff59850950beb39906dc1636b3ee7b6390f2086
4732f025a2a69f6c40787854c5da122689702f00f4f423061bb30ab7fa1e98d3
5381b2a7a77448c4908f5c79d21631f56c88ead0365981cac1dcaafe493c313e
53e9511401000f61c9d910b92cd6d5a58e38ae541975135944885e53fa91ecb7
5dfbd8cf98ebd4977d4f240dcabd5cd67b936c0095c2d5b9a77896daea877df6
5eebdb584a1acd6aacc36c59c22ec51bbd077d2dbbe0890b52e62fa6fb9cf784
5ff742e134e3d17ec7abea435f718e8f5603b95e7984e024b2310ac9ef862ddf
60ff43424c0ba9dc259ab32405345ef325a4cb4d0baf0c0b0c13f9d3672e99eb
68c6411cc9afa68047641932530cf7201f17029167d4811375f1458cae32c7bd
6b2c41b42f75e64d435ba56c2f2b6d79a11b862a2d994487dab3e51e298bc5c9
6b93b7372941a09f1ea69f8b71c5c4e211ea0f8a24061e702002ca84457bcddd
6d0857a9c77f9c5f2a5e6921e1cb9f7e1a5d6b947ad63b364d291157d3f840fb
70f3a6fdbbc5e2ae79c28b48b6478ee3c8ea6f2b705ca9dc9bf8e63a4f6e0c8d
72baf2ecb0a9df607e54b64c0925ffc6739ab5a8b18900bf5c1930bcc799395d
748d546c6db44f6aa4bbb8e586d79f56c63fa87580eb19a0f2d5079cbe0952b7
79040421b5a48dcc6e611dfe187b2f3e355791ad8511adb84f5c0948aa1d6c89
797ae2dbb2c538710fefe75dbe380b9f55b614cb03c4ae09bb3172e8234dd9d9
7a73ae8cca6ce6fa88f89d6154811cb453d6e6db9fa8ed5fbdaf8895aae601a5
7b19538dcf6d4bb84590c458f09c5707c8db53a42861fa56533c49c1a3acd953
7e3634bfd66e601d7585b237437f11f7d614b33705ba5f7bd75ab176c8250d38
858dfa529b960c6f6226b53beb55ba1900d3f498ba7be40724ed5c16d7d5a44b
871e5629d9c8898babf3ed579586e3f5f94a6c4623d3a0a7f9a99bf9d95ffc7b
8763749fd09245e7fa8c0ee2cc797d5520a9ef5d6846f044a0cd7c969c4bd7d4
89d839bbdc786c006304f3c6c6939150380aaa9e84d82bc31cdf0cf7609a6243
8b21fbd40c89763f51d5e06680c0971623500f4724c25958446bac794797057b
8baebd525324297faf86639266060172ded963767c832a609a991fa92c8463ab
8d1ed904d90e08048f42cdc9a25c2159f0f8dc4aa9dc01b0207645ea53abe189
957ab8417606ad41ad31f006d997af3f647dd5215af899551d08b3b472a4bc85

a0332fe0baa316fe793e757f9cf5938b099e97dc4624ead6f3bad8555c8a419b
a1482e62ecc89696a75adea7052c2e98a75c9d37304723abd110d60962bafdb7
a28d0c82a2a37462c2975b5eda7f91e8fc3c2ed50abfe357948ec4faabbd4951
a6637685091835826e62af279cc6c648188797f9edc05a2399a6686349102774
a6f1f68827303e655488c8d54b3be3ce8b1097f3ff374a2e4bc82ff96812781c
abc5b2118bc1d8c82f3726a5e30cf22ae3fa1c572dd3327b281ea6fd97ae9c06
afc45cc0df7f7e481bff45c6f62a6418b6ae4c8b474ec36113e05ab7ca7e2743
b1f91355a8472e364e07f05dc69bbd9c74dc1943e9c4475f46c2b448bb6d6e5d
b2b7218c3f649b9077510aac309357e884c314e0f488abed391415defb249f4c
b6b685fe020c481161060df9dbef0fc205cde479056c18aaeae184daa3f8a9c0
b784301cb2edafea875f779cf24e018f06732561069f6c4c3d86548029671642
ba557bd6b2c1d3297b2c9bd7294e47b9ad9ec6a937cddc879dd563c61a9abcbd
bb451151e52f0868f98e32d26ffa7c2be412b47cd470bf90d3cfe777b4a19f85
bd39f32177dc7a20f5087c5460ebf589035d9051336c69f07a26398f76aec40e
bf37542e9eb7a3b2f51d107e56d7551e6248f06ce18918e3dda2ebe9da1b0e80
bf97c4ff35b5e2c039aa1f1a9a164b7ec4d9339a631c84910b9a4d03b7927b8a
c2ba0018de8dcf0abfb2669cce95ed09377e9a9da7ff8e74e95688c99a025634
c3d797e67edf0dd435808f2f79ff4bfd0cf9177307f4a112b7da09f7dfdd8f2e
c441afb337c4803eed20ae255fbad3cdfac2800475c51e00a55369909efb4c89
cc6ad344d30178e04e49ab16cd43744925676562aded051835fb3f73401f31fa
ceab18331f785d0bf215f551b90f00567e36d339ba8e3ed8e45c0ad410b25808
d02a1eb597c66b602ac7d55095f771345ff5e90905ea12e523df2095030752b6
d6142f48664208710bab9fcab8dfcda66ad75ad756d2ce9c3aa243dcbc29bf4a
d665a8547baf067f2216821ecd4145eab1c75868f024d09140fb265b819d5194
d8d2092e174240d7bac63a9e1c199b442e1cb0f39d7fa32510b1aa7717c3ae38
e24de02415946133176b66017d54a5dcd7270c83f5ef01d79faff4e64d13c63b
e5502722c2bb84876903549445534c47cdaa586a0bb1e5b3a53162d75cc6cb28
e66ae0ac443b5140a1b35b5aaa6899eea296d9d633988eb044a395a34a887431
e92e01977d85f6834f57bd09e29e654b10da798844e4a64470cb22dac78bef93
e9723a2a9ca45787c35b864605a6be71ccf12b2d96dad8e7fc39117f7ba29abb
f28bb7bc5c801d5444ba6816e3a91d5bfaf0307578b7a1529415fc220fd9e9e8
f86b6aa11a276c24dd80db48f43c8a2f0c8df6e5426a7a0fee322c0427421ebb

“Type 1” Staging Server IP Addresses:
77[.]83[.]199[.]3
77[.]83[.]199[.]15
77[.]83[.]199[.]31
77[.]83[.]199[.]42
77[.]83[.]199[.]73
77[.]83[.]199[.]82
77[.]83[.]199[.]88
77[.]83[.]199[.]90
77[.]83[.]199[.]112
77[.]83[.]199[.]123
77[.]83[.]199[.]132
77[.]83[.]199[.]142
77[.]83[.]199[.]170
79[.]141[.]160[.]24
79[.]141[.]160[.]34
79[.]141[.]161[.]50
79[.]141[.]161[.]171
79[.]141[.]162[.]35
79[.]141[.]162[.]37

79[.]141[.]162[.]50
79[.]141[.]162[.]132
79[.]141[.]162[.]149
79[.]141[.]162[.]169
79[.]141[.]162[.]177
79[.]141[.]162[.]181
79[.]141[.]162[.]187
79[.]141[.]162[.]204
79[.]141[.]162[.]229
79[.]141[.]163[.]138
79[.]141[.]163[.]176
79[.]141[.]172[.]204
79[.]141[.]172[.]223
79[.]141[.]172[.]229
79[.]141[.]172[.]232
79[.]141[.]172[.]240
79[.]141[.]173[.]60
79[.]141[.]173[.]161
79[.]141[.]173[.]168
85[.]158[.]111[.]29
85[.]158[.]111[.]38
85[.]158[.]111[.]53
85[.]158[.]111[.]75
85[.]158[.]111[.]81
85[.]158[.]111[.]126
89[.]46[.]38[.]34
89[.]46[.]38[.]48
89[.]46[.]38[.]88
89[.]169[.]12[.]48
91[.]193[.]19[.]32
91[.]193[.]19[.]64
91[.]193[.]19[.]78
91[.]193[.]19[.]127
91[.]193[.]19[.]163
91[.]193[.]19[.]188
91[.]193[.]19[.]190
98[.]142[.]240[.]165
98[.]142[.]240[.]188
98[.]142[.]240[.]214
98[.]142[.]240[.]221
98[.]142[.]240[.]246
98[.]142[.]251[.]26
98[.]142[.]251[.]32
98[.]142[.]251[.]42
98[.]142[.]251[.]53
185[.]33[.]84[.]131
185[.]33[.]84[.]153
185[.]33[.]84[.]169
185[.]33[.]85[.]20
185[.]33[.]85[.]26
185[.]33[.]85[.]33
185[.]33[.]85[.]38
185[.]33[.]85[.]52

185[.]33[.]86[.]37
193[.]42[.]38[.]11
193[.]42[.]38[.]79
193[.]42[.]38[.]85
193[.]42[.]38[.]86
193[.]111[.]208[.]2
193[.]111[.]208[.]17
193[.]111[.]208[.]19
193[.]111[.]208[.]23
193[.]111[.]208[.]24
193[.]111[.]208[.]46
193[.]111[.]208[.]75
193[.]111[.]208[.]97
193[.]111[.]208[.]100

Additional IP Addresses Likely Linked to "Type 1" Staging Infrastructure:
23[.]140[.]40[.]66
45[.]153[.]191[.]245
46[.]29[.]163[.]28
89[.]169[.]12[.]48
89[.]253[.]222[.]25
89[.]253[.]222[.]156
95[.]182[.]123[.]86
185[.]231[.]245[.]158
217[.]114[.]15[.]253

"Type 2" Staging Server IP Addresses:
45[.]61[.]134[.]76
77[.]83[.]199[.]162
79[.]141[.]162[.]135
79[.]141[.]163[.]169
91[.]193[.]19[.]220
144[.]172[.]115[.]211
172[.]86[.]90[.]84
185[.]33[.]86[.]11
185[.]80[.]53[.]79
194[.]15[.]216[.]118

"Type 2" Staging Server Domains:
filmlerzltyazilimsx[.]shop
foolowme[.]com
joiner[.]best
lowi1[.]com
morniksell[.]com
persistancejs[.]store
pomofight[.]com
port4loms[.]com
signaturepl[.]com
yungask[.]com

Domains Linked to oreshnik[@]mailum[.]com:
108zhao[.]shop
1sou[.]top

6hms[.]top
789pettoys[.]shop
7serv[.]top
99wc[.]top
abocamuseum[.]icu
actionmovies[.]top
alcmz[.]top
alhasba[.]com
amxdh1[.]icu
anoteryo[.]top
arearugs[.]top
as5yo[.]top
ashesplayer[.]top
avodaride[.]top
azyaamode[.]shop
baihao[.]shop
baihuah[.]top
bedoueroom[.]top
bestproductreviews[.]xyz
bestrollerballpen[.]top
blogdojhow[.]com
bnpparibas[.]top
bokra[.]top
bond007[.]xyz
boxworld[.]top
bstionline[.]com
buildingjobs[.]xyz
buscavuelosbaratos[.]top
buyedmeds[.]top
buylisinopril[.]top
celebrex[.]top
chaojiwang[.]top
chenyiwen[.]top
chinapark[.]top
christianlouboutin2017[.]top
cialissale[.]top
cinselurunler[.]xyz
coinseasygenerator[.]top
couterfv[.]top
couturella[.]shop
covaticonstructioncorp[.]shop
cozartan[.]top
cryptohardware[.]shop
dcdh4[.]shop
dealermobil[.]top
depechemode[.]shop
directoryframework[.]top
discountmontblanc[.]top
discoveronline[.]top
doodstream[.]shop
downloadfreak[.]top
erectilehelp[.]top
filmezz[.]top

filmlerzltyazilimsx[.]shop
fjs95[.]shop
fmovies123[.]top
forging[.]top
fragzone[.]top
franquicias[.]top
fuckhdmov[.]top
gededewe[.]shop
getin[.]top
glitterygadgets[.]shop
gmartph[.]shop
gmt-a[.]shop
grandzxc[.]bet
guosong[.]top
haidao10[.]top
headtechnologies[.]xyz
healthcareplans[.]top
heim-k[.]shop
helperection[.]top
hilfe-ed[.]top
hirek[.]top
howtogetaloan[.]top
ida-ci[.]com
islighting[.]top
iwine[.]top
izone[.]digital
jerseysus[.]top
jiezishijie[.]top
jkse[.]shop
jsmakert[.]shop
k2bsc[.]top
kaestner[.]top
kamagrafr[.]icu
kanshuwang[.]top
kazumaka[.]top
kfzversicherungskosten[.]top
khusinhthaidanphuong[.]top
kingdomholding[.]top
krediteonlinevergleichen[.]top
lang3666[.]top
langwonet[.]top
layardrama21[.]top
lebensversicherungvergleich[.]top
levciavia[.]top
linhua97[.]top
linksoflondononsale[.]top
linksoflondonsale[.]top
liruo[.]top
liveskortv[.]shop
loanonline[.]top
loispaigesimenson[.]com
losartan[.]top
lovedou[.]top

```
lqsword[.]top
lx7v9[.]top
lycosex[.]top
machine-a-plastifier[.]com
manwithedhelp[.]top
marmocer[.]top
mbpen163[.]top
medicamentsbonmarche[.]top
meimei68[.]top
menjimmychooonline[.]top
milebox[.]shop
mindsetgrowth[.]shop
mm37[.]icu
monclerjackets[.]top
moruk[.]xyz
motocyclenews[.]top
moviefone[.]top
moviesone[.]top
movtime76[.]shop
movtime78[.]shop
musicdownloader[.]top
my-privatebanker[.]top
mybeststream[.]xyz
nackt-bilder[.]top
nana44[.]shop
newbalancesport[.]top
palcomp3[.]top
parisforrent[.]top
pasangiklan[.]top
patekphillipwatches[.]top
pielsteel[.]top
pravaix[.]top
rag382[.]top
rasin[.]shop
refanprediction[.]shop
regopramide[.]top
rnsddse[.]top
sales2016[.]top
sdnews[.]top
searchgo[.]shop
searchweb[.]top
semikeren[.]icu
simvascor[.]icu
simvascor[.]top
snapcans[.]top
sneakermall[.]top
soap2dayfree[.]top
socialsignals[.]shop
socksforrocks[.]shop
streaming-films[.]xyz
syavsp5[.]top
tdsc[.]top
techradar[.]top
```

tiffanyearringforwomen[.]top
todoarmarios[.]top
todocalefactores[.]top
todocarritos[.]top
travelplace[.]top
trendings[.]top
universaltechnology[.]top
uochut[.]shop
via345[.]top
villahome[.]top
viloriterso[.]icu
viptravelcentres[.]com
vog168[.]top
wandan[.]top
wap9[.]top
warpdrive[.]top
watchesbest[.]top
wavob[.]top
wdwnp[.]top
xelesex[.]top
ydh7[.]shop
yntz6[.]shop
yourcialsupply[.]top
youtubevideo[.]top
yxta[.]top
yybvf[.]top
zaheirx[.]shop
zakachka[.]top
zerolendnow[.]top
zt45gg[.]top

Compromised Law Firm Websites:
bianchilawgroup[.]com
brattonlawgroup[.]com
brighterdaylaw[.]com
defensegroup[.]com
dwicriminallawcenter[.]com
fisherstonelaw[.]com
jarrettfirm[.]com
raineyandrainey[.]com
rbbfirm[.]com
rmvlawyer[.]com
www[.]brentadams[.]com
www[.]cfblaw[.]com
www[.]gerlinglaw[.]com
www[.]immigration-defense[.]com
www[.]schwartzandschwartz[.]com

Sectop RAT Hash:
59e7e7698d77531bfbfea4739d29c14e188b5d3109f63881b9bcc87c72e9de78

SecTopRAT C2 IP Address:
85[.]158[.]110[.]179[:]15847

Other Hashes:
5f1bd92ad6edea67762c7101cb810dc28fd861f7b8c62e6459226b7ea54e1428

Email Address Linked to GrayCharlie:
oreshnik[@]mailum[.]com

Appendix B: "Type 1" Staging Infrastructure

IP Address	ASN	Organization
77[.]83[.]199[.]3	AS202015	HZ Hosting Ltd
77[.]83[.]199[.]15	AS202015	HZ Hosting Ltd
77[.]83[.]199[.]31	AS202015	HZ Hosting Ltd
77[.]83[.]199[.]42	AS202015	HZ Hosting Ltd
77[.]83[.]199[.]73	AS202015	HZ Hosting Ltd
77[.]83[.]199[.]82	AS202015	HZ Hosting Ltd
77[.]83[.]199[.]88	AS202015	HZ Hosting Ltd
77[.]83[.]199[.]90	AS202015	HZ Hosting Ltd
77[.]83[.]199[.]112	AS202015	HZ Hosting Ltd
77[.]83[.]199[.]123	AS202015	HZ Hosting Ltd
77[.]83[.]199[.]132	AS202015	HZ Hosting Ltd
77[.]83[.]199[.]142	AS202015	HZ Hosting Ltd
77[.]83[.]199[.]170	AS202015	HZ Hosting Ltd
79[.]141[.]160[.]24	AS202015	HZ Hosting Ltd
79[.]141[.]160[.]34	AS202015	HZ Hosting Ltd
79[.]141[.]161[.]50	AS202015	HZ Hosting Ltd
79[.]141[.]161[.]171	AS202015	HZ Hosting Ltd
79[.]141[.]162[.]35	AS202015	HZ Hosting Ltd
79[.]141[.]162[.]37	AS202015	HZ Hosting Ltd
79[.]141[.]162[.]50	AS202015	HZ Hosting Ltd
79[.]141[.]162[.]132	AS202015	HZ Hosting Ltd
79[.]141[.]162[.]149	AS202015	HZ Hosting Ltd
79[.]141[.]162[.]169	AS202015	HZ Hosting Ltd

IP Address	ASN	Organization
79[.]141[.]162[.]177	AS202015	HZ Hosting Ltd
79[.]141[.]162[.]181	AS202015	HZ Hosting Ltd
79[.]141[.]162[.]187	AS202015	HZ Hosting Ltd
79[.]141[.]162[.]204	AS202015	HZ Hosting Ltd
79[.]141[.]162[.]229	AS202015	HZ Hosting Ltd
79[.]141[.]163[.]138	AS202015	HZ Hosting Ltd
79[.]141[.]163[.]176	AS202015	HZ Hosting Ltd
79[.]141[.]172[.]204	AS202015	HZ Hosting Ltd
79[.]141[.]172[.]223	AS202015	HZ Hosting Ltd
79[.]141[.]172[.]229	AS202015	HZ Hosting Ltd
79[.]141[.]172[.]232	AS202015	HZ Hosting Ltd
79[.]141[.]172[.]240	AS202015	HZ Hosting Ltd
79[.]141[.]173[.]60	AS202015	HZ Hosting Ltd
79[.]141[.]173[.]161	AS202015	HZ Hosting Ltd
79[.]141[.]173[.]168	AS202015	HZ Hosting Ltd
85[.]158[.]111[.]29	AS202015	HZ Hosting Ltd
85[.]158[.]111[.]38	AS202015	HZ Hosting Ltd
85[.]158[.]111[.]53	AS202015	HZ Hosting Ltd
85[.]158[.]111[.]75	AS202015	HZ Hosting Ltd
85[.]158[.]111[.]81	AS202015	HZ Hosting Ltd
85[.]158[.]111[.]126	AS202015	HZ Hosting Ltd
89[.]46[.]38[.]34	AS202015	HZ Hosting Ltd
89[.]46[.]38[.]48	AS202015	HZ Hosting Ltd
89[.]46[.]38[.]88	AS202015	HZ Hosting Ltd
89[.]169[.]12[.]48	AS207957	SERV.HOST GROUP LTD

IP Address	ASN	Organization
91[.]193[.]19[.]32	AS202015	HZ Hosting Ltd
91[.]193[.]19[.]64	AS202015	HZ Hosting Ltd
91[.]193[.]19[.]78	AS202015	HZ Hosting Ltd
91[.]193[.]19[.]127	AS202015	HZ Hosting Ltd
91[.]193[.]19[.]163	AS202015	HZ Hosting Ltd
91[.]193[.]19[.]188	AS202015	HZ Hosting Ltd
91[.]193[.]19[.]190	AS202015	HZ Hosting Ltd
98[.]142[.]240[.]165	AS202015	HZ Hosting Ltd
98[.]142[.]240[.]188	AS202015	HZ Hosting Ltd
98[.]142[.]240[.]214	AS202015	HZ Hosting Ltd
98[.]142[.]240[.]221	AS202015	HZ Hosting Ltd
98[.]142[.]240[.]246	AS202015	HZ Hosting Ltd
98[.]142[.]251[.]26	AS202015	HZ Hosting Ltd
98[.]142[.]251[.]32	AS202015	HZ Hosting Ltd
98[.]142[.]251[.]42	AS202015	HZ Hosting Ltd
98[.]142[.]251[.]53	AS202015	HZ Hosting Ltd
185[.]33[.]84[.]131	AS202015	HZ Hosting Ltd
185[.]33[.]84[.]153	AS202015	HZ Hosting Ltd
185[.]33[.]84[.]169	AS202015	HZ Hosting Ltd
185[.]33[.]85[.]20	AS202015	HZ Hosting Ltd
185[.]33[.]85[.]26	AS202015	HZ Hosting Ltd
185[.]33[.]85[.]33	AS202015	HZ Hosting Ltd
185[.]33[.]85[.]38	AS202015	HZ Hosting Ltd
185[.]33[.]85[.]52	AS202015	HZ Hosting Ltd
185[.]33[.]86[.]37	AS202015	HZ Hosting Ltd

IP Address	ASN	Organization
193[.]42[.]38[.]11	AS202015	HZ Hosting Ltd
193[.]42[.]38[.]79	AS202015	HZ Hosting Ltd
193[.]42[.]38[.]85	AS202015	HZ Hosting Ltd
193[.]42[.]38[.]86	AS202015	HZ Hosting Ltd
193[.]111[.]208[.]2	AS202015	HZ Hosting Ltd
193[.]111[.]208[.]17	AS202015	HZ Hosting Ltd
193[.]111[.]208[.]19	AS202015	HZ Hosting Ltd
193[.]111[.]208[.]23	AS202015	HZ Hosting Ltd
193[.]111[.]208[.]24	AS202015	HZ Hosting Ltd
193[.]111[.]208[.]46	AS202015	HZ Hosting Ltd
193[.]111[.]208[.]75	AS202015	HZ Hosting Ltd
193[.]111[.]208[.]97	AS202015	HZ Hosting Ltd
193[.]111[.]208[.]100	AS202015	HZ Hosting Ltd

Appendix C: MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Reconnaissance: Gather Victim Host Information: Client Configurations	T1592.004
Resource Development: Acquire Infrastructure: Domains	T1583.001
Resource Development: Acquire Infrastructure: Virtual Private Server	T1583.003
Resource Development: Acquire Infrastructure: Server	T1583.004
Resource Development: Acquire Access	T1650
Initial Access: Phishing: Spearphishing Link	T1566.002
Initial Access: Phishing: Spearphishing Attachment	T1566.001
Initial Access: Exploit Public-Facing Application	T1190
Execution: Command and Scripting Interpreter: PowerShell	T1059.001
Execution: User Execution: Malicious File	T1204.002
Execution: User Execution: Malicious Copy and Paste	T1204.004
Execution: Command and Scripting Interpreter: Windows Command Shell	T1059.003
Execution: User Execution: Malicious Link	T1204.001
Execution: Command and Scripting Interpreter: JavaScript	T1059.007
Persistence: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
Defense Evasion: Masquerading	T1036
Defense Evasion: Obfuscated Files or Information	T1027
Defense Evasion: Obfuscated Files or Information: Compression	T1027.015
Discovery: Permission Groups Discovery: Domain Groups	T1069.002
Collection: Clipboard Data	T1115
Command and Control: Ingress Tool Transfer	T1105
Command and Control: Remote Access Tools	T1219
Command and Control: Application Layer Protocol: Web Protocols	T1071.001

Appendix D: Sigma Rules

```
title: NetSupport client32.exe Execution from Non-Standard Path
id: 436b7c13-114d-4012-82f9-17ade263dba6
status: stable
description: Detects execution of NetSupport Manager client (client32.exe) where the image
path contains "NetSupport" but is not in the standard Program Files locations.
references:
    - https://tria.ge/250214-dmwwlazmgn
author: IPER, Insikt Group, Recorded Future
date: 2025-11-13
level: high
tags:
    - attack.t1219 # Remote Access Tools
logsource:
    product: windows
    category: process_creation
detection:
    client32:
        Image|endswith: 'client32.exe'
        Image|contains: 'NetSupport'
    legitimate_paths:
        Image|startswith:
            - 'C:\Program Files\NetSupport Manager\'
            - 'C:\Program Files (x86)\NetSupport Manager\'
    condition: client32 and not legitimate_paths
falsepositives:
    - Unlikely
```

Appendix E: YARA Rules

```
rule MAL_Dropper_NetSupportRAT {
    meta:
        author = "TTPMNL, Insikt Group, Recorded Future"
        date = "2025-11-17"
        description = "Detects a dropper that delivers a decoy ChaGPT Installer and
NetSupport RAT"
        version = "1.0"
        reference = "https://x.com/ShadowOpCode/status/1968611205280338187"
        reference = "https://tria.ge/250918-epjvgshr4y/behavioral1"
        hash = "d86f647f3dfa6a53de7b531cb590636331f83afcea60d4b3d44de5ea3b7d33af"
        malware = "NetSupport"
        malware_id = "TWOU5d"
        category = "MALWARE"
    strings:
        //dropped files
        $d1 = "ChatGPT Installer.exe"
        $d2 = "setup.exe"
        //netsupport strings
        $n1 = "NetSupport" nocase
        $n2 = "install_netsupport_manager_silently"
        $n3 = "is@netsupportsoftware.com"

    condition:
        uint16(0) == 0x5A4D and
        all of ($d*) and
        2 of ($n*)
}
```

Appendix F: Snort Rules

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"Outbound NetSupport RAT C2
Communication"; flow:to_server,established; content:"POST"; nocase; content:"User-agent:
NetSupport Manager"; nocase; fast_pattern; content:"CMD=/"; nocase;
reference:url,https://www.virustotal.com/gui/file/49a568f8ac11173e3a0d76cff6bc1d4b9bdf2c35
c6d8570177422f142dcfdbe3/detection; classtype:bad-unknown; sid:52460001; rev:2;
metadata:author Insikt Group/JET, created_at 2019-12-16, updated_at 2024_07_06,
mitre_tactic_id TA0011, mitre_tactic_name Command-And-Control;)
```

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 intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com