
ABOUT

We are a small organized crime group operating out of Finland. While our scale may be modest, our reach is not — our services have been used worldwide, with clients as far away as Japan. Our focus is on providing online-based services. We began this operation in December 2023, and since then we have generated approximately $41,000 in revenue. We use U.S. dollars rather than euros to make international transactions smoother — professionalism has no borders. In May of this year, we temporarily suspended all of our services. After careful consideration, we relaunched them this Monday. One significant change is in our payment method: instead of cryptocurrency, we now accept PayPal transfers directly. This adjustment was made to improve accessibility — after all, crime should be inclusive. We are also developing a dedicated dark web platform, although its release depends on our colleague's availability to complete the programming. Until then, we will continue to operate as we are now, fully aware of the risks involved. But yeah, as mentioned, all payments are now processed through PayPal.

We provide online lessons (phishing, frauds), hacking services (social media etc.), pre-made viruses, etc. Whatever you can imagine. You can also request a service via email.

Once you have selected the services you wish to purchase, please send us an email including the number of each service, along with any personal requests you would like us to include.
The prices listed on this site are only indicative; the final price will be determined based on your order. You will receive your order approximately 1–24 hours after payment. The delivery can be sent to any email address of your choice - just let us know which one.

Our email: aaapm.vittu@proton.me xxx Tara, your personal assistant . <3

LESSONS

PHISHING

1.Email phishing: Sending an email with a malicious link or attachment to trick users into revealing sensitive information or downloading malware 20$

2. Spear phishing: A more targeted approach than general email phishing, it involves sending tailored emails to specific individuals within an organization, using personal information to appear more legitimate and trustworthy 25$

3. Whaling: A specific type of spear-phishing that targets high-profile individuals within an organization, such as CEOs, CFOs, or other senior executives, to gain access to high-level data 25$

4. Smishing: Phishing attacks carried out via SMS text messages, containing malicious links or urgent requests to share personal information 15$

5. Vishing: Attackers use phone calls, or pre-recorded robocalls, to trick victims into revealing confidential information or providing login details 35$

6. Social media phishing: Attackers use popular social media platforms like Facebook, Instagram, or LinkedIn to send malicious messages or create fake profiles to lure victims into providing information or clicking on harmful links 20$

7. Angler phishing: A method that uses social media by creating fake customer service accounts to intercept customer complaints and try to trick them into revealing login information 20$

8. Clone phishing: Involves taking a previously delivered, legitimate email and creating a nearly identical copy, then changing a link or attachment to be malicious, making it more likely for a victim to click 25$

9. Pharming: A deceptive attack where malicious code is installed on a victim's device, or a malicious website is created, that redirects users to a fake version of a legitimate site even when they type the correct URL 30$

10. Evil twin phishing: Occurs when an attacker sets up a fake, unsecured Wi-Fi network in a public place that looks like a legitimate one. Users who connect to this "evil twin" can have their data intercepted 40$

FRAUDS

11. Identity Theft: Steal personal and financial data to impersonate someone, open accounts, or commit crimes in their name 25$

12. Advance Fee Fraud: Victims are promised a large sum of money, a valuable prize, or a good service, but must first pay a fee or taxes upfront, which never materialize 25$

13. Lottery, Sweepstakes, and Competition Scams: Similar to advance fee fraud, victims are told they've won a prize but must pay a fee to claim it 25$

14. Imposter Scams: Scammers pretend to be a trusted authority figure, such as a government official, family member in distress, or even a tech support representative, to get the victim to send money or provide information 25$

15. Job and Employment Scams: Offer fake job opportunities or business ventures from which the victim is asked to pay for training or equipment before working or starting the business 25$

16. Investment Fraud: Schemes like Ponzi schemes and pyramid schemes lure victims with the promise of high returns but are unsustainable and rely on money from new investors to pay earlier ones 25$

17. Credit Card Fraud: Using stolen or fraudulent credit card details to make unauthorized purchases 20$

18. Insurance Fraud: Falsifying claims or details to collect money from an insurance company 25$

19. Corporate Fraud: Involves manipulation of financial statements, misappropriation of assets, or corruption within a business 40$

SERVICES

HACKING

20. Email hacking 20$

21. Facebook hacking 20$

22. Instagram hacking 20$

23. Website hacking 25$

24. Cell phone hacking,

- iphone 35$

-android 30$

25. Search engine hacking 35$

26. Ip-address tracking 15$

VIRUSES ETC.

You need to copy the text from the screenshots that our colleague has programmed the virus into. In addition, you need to finalize and verify the functionality of the virus yourself, but don't worry, we will send you an easy and detailed guide to creating each virus. This is because we cannot directly send the virus to you to copy, so that the virus does not activate on your device.

27.Viruses: A type of malware that inserts itself into legitimate software or files and spreads when the infected file is executed, corrupting data and software 30$

28.Worms: Unlike viruses, worms are self-replicating and can spread independently across networks, often exploiting system vulnerabilities to install themselves on other devices 30$

29. Trojans (Trojan Horses): These disguise themselves as legitimate or desirable programs to trick users into installing them. Once executed, they can perform malicious actions like stealing data or giving attackers remote control 30$

30. Ransomware: This malware encrypts a user's data or locks their system and demands a ransom payment to restore access 30$

31. Spyware: Collects user information without their knowledge or consent. This can include passwords, credit card details, and browsing habits 35$

32. Rootkits: A set of tools that gives an attacker hidden control over a system. They are designed to evade detection by hiding their presence and other malware 3$

33. Adware: Displays unwanted advertisements on a user's device, often appearing as pop-up windows or redirects 30$

34. Bots and Botnets: A bot is a software program designed to perform automated tasks, often on a network of infected computers (a botnet) controlled by a single attacker. These are used for various malicious activities, like launching DDoS attacks 30$

35. Keyloggers: A specific type of spyware that records every keystroke a user types, capturing sensitive information like passwords and financial details 30$

36. Key Differences: The main distinctions between these types of malware lie in their method of infection and their primary function 30$

37. Infection: Viruses require a host file, while worms self-replicate and spread autonomously. Trojans use deception to get installed. 30$

38. Activity: Some malware, like ransomware, aims to disrupt or extort money, while others, like spyware, focus on information theft. 30$

More services and lessons coming soon. Feel free to request or share ideas of services that we could provide. Also feedback is more than okay, send it to our email aaapm.vittu@proton.me

Also forgive us for poor english!