

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA : Hon. Madeline Cox Arleo
 :
 v. : Crim. No. 16-
 :
 VADYM IERMOLOVYCH : 18 U.S.C. § 1349,
 a/k/a "Vadim Ermolovich," : 18 U.S.C. § 371, and
 a/k/a "Dima Ermolovich," : 18 U.S.C. § 1028A(a)(1)
 a/k/a "Dim," :
 a/k/a "Dima," :
 a/k/a "Dingos777," :
 a/k/a "Vaer," :
 a/k/a "Nadal," :
 a/k/a "PriestTF," and :
 a/k/a "Kamazik" :

INFORMATION

The defendant having waived in court prosecution by indictment, the United States Attorney for the District of New Jersey charges:

INTRODUCTION

1. From in or about February 2010 through in or about November 2014, VADYM IERMOLOVYCH, together with others (the "Conspirators"), engaged in an international computer hacking and wire fraud scheme whereby they: (a) hacked into the computer networks of Marketwired L.P., PR Newswire Association LLC, and Business Wire (collectively, the "Victim Newswires"); (b) stole confidential press releases containing material nonpublic information from the Victim Newswires' internal computer networks prior to their public release (the "Stolen Releases"); and (c) traded ahead of the material nonpublic information contained in the Stolen Releases before its distribution to the investing public. During the course of the scheme, the Conspirators accessed

more than 150,000 Stolen Releases and executed profitable trades based on the material nonpublic information contained in the Stolen Releases. In total, the scheme generated more than \$30 million in illicit trading profits.

Relevant Individuals and Entities

2. At all times relevant to this Information,
 - a. Defendant VADYM IERMOLOVYCH (“IERMOLOVYCH”), a/k/a “Vadim Ermolovich,” a/k/a “Dima Ermolovich,” a/k/a “Dim,” a/k/a “Dima,” a/k/a “Dingos777,” a/k/a “Vaer,” a/k/a “Nadal,” a/k/a “PriestTF,” and a/k/a “Kamazik,” was a computer hacker who resided in Ukraine.
 - b. Co-conspirator Ivan Turchynov, a/k/a “Ivan Turchinov,” a/k/a “Ivan Turchinoff,” a/k/a “Vladimir Gopienko,” a/k/a “DSU,” was a computer hacker who resided in Ukraine.
 - c. Co-conspirator Oleksandr Ieremenko, a/k/a “Aleksandr Eremenko,” a/k/a “Zlom,” a/k/a “Lamarez,” was a computer hacker who resided in Ukraine.
 - d. At various times relevant to this Information, IERMOLOVYCH, Turchynov, and Ieremenko (collectively the “Hackers”) worked together to breach the networks of the Victim Newswires.
 - e. At various times relevant to this Information, certain traders (the “Traders”), either opened, maintained, controlled, benefitted from, or were designated as authorized traders, on a number of brokerage accounts in which trades made in furtherance of the scheme were executed.

f. At all times relevant to this Information, the Victim Newswires included the following entities, including any predecessor entities: Marketwired L.P. (“Marketwired”), which was headquartered in or around Toronto, Canada; PR Newswire Association LLC (“PRN”), which was headquartered in or around New York, New York, and maintained and utilized computer servers located in the District of New Jersey that were affected by the unlawful activity discussed below; and Business Wire, which was headquartered in or around San Francisco, California. The Victim Newswires were in the business of, among other things, issuing press releases on behalf of publicly traded companies (the “Issuers”).

g. Generally, the Victim Newswires maintained contractual relationships with the Issuers, pursuant to which the Issuers provided confidential press releases to the Victim Newswires, which maintained them on their computer servers for a period of time until their distribution to the public. The Victim Newswires finalized and released the press releases to the public at the direction of, or in consultation with, the Issuers. The press releases typically contained material nonpublic information concerning, among other things, the Issuers’ financial performance, quarterly earnings, year-end earnings, and potential mergers or acquisitions involving the Issuers. As a result, maintaining the confidentiality of this information prior to its public release was critical to the operations of the Victim Newswires and to the Issuers. Indeed, the Victim Newswires and the Issuers had the right to control the use of the confidential and economically valuable business information

contained in the press releases, including determining when and how the information would be disclosed to the investing public. Accordingly, the Victim Newswires maintained press releases on restricted, nonpublic servers prior to distributing the final press releases.

h. At all times relevant to this Information, “Employee #1” was an employee of PR Newswire.

Relevant Hacking Terms

i. “Brute Force Attacks” or “bruting” referred to decrypting data by running programs that systematically checked all possible passwords until the correct password was revealed. Among other things, this methodology could be used to decrypt “password hashes,” which were strings of encrypted data generated when a password was passed through an encryption algorithm. Passwords for network accounts were often stored on networks as password hashes as a security measure.

j. “Internet Protocol (IP) addresses” were unique numeric addresses assigned to every Internet connection. Every device connected to the Internet was assigned an IP address in order to send and receive communications with other devices or services available on the Internet.

k. “Malware” was malicious software programmed to, among other things, gain unauthorized access to computers; identify, store, and export information from hacked computers; and to evade detection of intrusions by anti-virus programs and other security features running on those computers.

l. “Reverse shells” were a specific type of malware designed to initiate a connection to an external computer from within a hacked computer network.

m. “Structured Query Language” or “SQL” was a computer programming language designed to retrieve and manage data in computer databases.

n. “SQL Injection Attacks” were methods of hacking into and gaining unauthorized access to computers connected to the Internet using a series of SQL instructions.

Overview of the Scheme

3. From in or about February 2010 through in or November 2014, the Hackers and others gained unauthorized access into the computer networks of the Victim Newswires and stole confidential press releases containing material nonpublic information prior to their public release. The Hackers then shared the Stolen Releases with, among others, the Traders using overseas computer servers. The Traders traded on the material nonpublic information contained in the Stolen Releases prior to their distribution to the investing public. The Traders paid the Hackers for access to the servers based, in part, on a percentage of how much money the Traders made trading ahead of the information contained in the Stolen Releases.

4. In executing the scheme, the Hackers and the Traders deprived the Victim Newswires and the Issuers of their right to control the use of the confidential and economically valuable business information contained in the

Stolen Releases, including the decision of when and how the information should be disclosed to the public.

5. In furtherance of the scheme, the Hackers and Traders obtained over 150,000 Stolen Releases, executed trades in advance of over approximately 800 of the Stolen Releases, and realized over \$30 million in illicit trading profits.

The Intrusions into the Victim Newswires

A. Marketwired

6. From in or about February 2010 through in or about November 2013, the Hackers gained unauthorized access to press releases on the networks of Marketwired using a series of SQL Injection Attacks. Between on or about April 24, 2012 and on or about July 20, 2012 alone, co-conspirator Turchynov sent SQL Injection Attack commands into the networks of Marketwired on at least 390 occasions.

7. The first theft of press releases from Marketwired's networks occurred at least as early as on or about February 26, 2010. After gaining access, the Hackers installed multiple reverse shells onto Marketwired's networks, which they used to facilitate their theft of data. In addition to sending SQL Injection Attack commands, in or about March 2012, the Hackers launched an intrusion into the networks of Marketwired whereby they obtained contact and log-in credential information for Marketwired's employees, clients, and business partners. The Hackers then misrepresented their identities by using these login credentials to gain access to confidential information,

including press releases, located on Marketwired's networks. From in or about February 2010 through in or about November 2013, the Hackers had access to the content of more than 100,000 press releases on the internal networks of Marketwired before they were released to the investing public. The Hackers continued to attempt to gain unauthorized access to Marketwired's networks until at least as late as in or about July 2015.

8. The Hackers shared the Stolen Releases by, among other methods, creating servers where the Stolen Releases could be accessed before they were publicly disseminated by the Victim Newswires. Defendant IERMOLOVYCH advertised one of these servers, which contained Marketwired Stolen Releases, on a criminal web forum and accepted tens of thousands of dollars in payments for granting access to the Stolen Releases.

B. PRN

9. The Hackers hacked into PRN's computer servers in the District of New Jersey on the following three occasions: from in or about July 2010 through in or about January 2011; from in or about July 2011 through in or about March 2012; and from in or about January 2013 through in or about March 2013. During these intrusions, the Hackers accessed and stole more than approximately 40,000 press releases before they were publicly disseminated.

10. On or about January 12, 2011, PRN changed its network infrastructure, which had the effect of cutting off the Hackers' access to its networks. As a result, between on or about January 12, 2011 and in or about

June 2011, the Hackers increased their activities within the networks of Marketwired, where they still maintained access at the time.

11. Between in or about July 2011 and in or about March 2012, the Hackers again accessed PRN's networks and installed malware on its servers. During this same time period, the Hackers' activities on the networks of Marketwired decreased, and they shifted their focus to PRN's networks.

12. Between on or about March 9, 2012 and on or about March 13, 2012, PRN identified and removed malware that the Hackers had installed on its servers, resulting in the Hackers once again losing their unauthorized access to PRN's networks.

13. Between on or about January 25, 2013 and on or about March 1, 2013, the Hackers regained unauthorized access to the networks of PRN. In order to gain this access, the Hackers, including defendant IERMOLOVYCH, purchased access to a large database of stolen credentials that was obtained through an intrusion into a social networking website. The Hackers then reviewed the database and collected usernames and logins for PRN employees (the "PRN Logins"). The Hackers, including defendant IERMOLOVYCH, then used the PRN logins to access the Virtual Private Network ("VPN") of PRN without authorization and obtained Stolen Releases, including by using the PRN username and password belonging to Employee #1 on or about February 27, 2013.

14. On or about March 1, 2013, PRN detected the intrusion and once again blocked the Hackers' unauthorized access to its networks. Consistent

with their prior patterns, after losing access to PRN's networks, the Hackers increased their activities on the networks of Marketwired.

C. Business Wire

15. From in or about March 2012 through in or about June 2012, the Hackers hacked into Business Wire and stole the login credentials of a number of Business Wire's employees in an effort to steal press releases from Business Wire prior to their public distribution. In or around 2012, and in furtherance of these efforts, defendant IERMOLOVYCH purchased access to the Business Wire network that was obtained by another hacker's successful SQL Injection Attack.

Count One
(Conspiracy to Commit Wire Fraud)

16. The allegations contained in paragraphs 1 through 15 of this Information are realleged and incorporated as though fully set forth in this paragraph.

The Conspiracy

17. From in or about February 2010 through in or about November 2014, in Bergen, Hudson, and Middlesex Counties, in the District of New Jersey and elsewhere, defendant

VADYM IERMOLOVYCH

did knowingly and intentionally conspire and agree with others to devise a scheme and artifice to defraud the Victim Newswires and the Issuers, and to obtain money and property, including the confidential business information of the Victim Newswires and the Issuers, by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice to defraud, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

Object of the Conspiracy

18. It was the object of the conspiracy for defendant IERMOLOVYCH and others to obtain money and property by means of fraudulently obtaining confidential business information from the Victim Newswires and the Issuers, namely, unreleased press releases containing material nonpublic information

concerning publicly traded companies – the Stolen Releases – and trading upon the material nonpublic information contained in the Stolen Releases ahead of its public distribution, thereby realizing and sharing in the proceeds of the profitable illegal trading.

Manner and Means of the Conspiracy

19. It was part of the conspiracy that the Hackers, including defendant IERMOLOVYCH, gained unauthorized access to the computer networks of the Victim Newswires by employing a variety of hacking methods, including the use of stolen login credentials, SQL Injection Attacks, and Brute Force Attacks. In some cases, to gain unauthorized access to the Victim Newswires' networks the Hackers illegally obtained the contact and login credential information for employees, clients, and business partners of the Victim Newswires. By employing these and other hacking methods, the Hackers misrepresented their identities in order to gain access to information on the internal networks of the Victim Newswires that was otherwise off limits to them.

20. It was further part of the conspiracy that after gaining unauthorized access to the computer networks of the Victim Newswires, the Hackers, including defendant IERMOLOVYCH, exfiltrated Stolen Releases containing confidential business information from those networks and stored them on servers they controlled.

21. It was further part of the conspiracy that the Hackers, including defendant IERMOLOVYCH, provided access to the servers on which they stored the Stolen Releases to, among others, the Traders.

22. It was further part of the conspiracy that the Traders and others executed profitable trades in brokerage accounts they controlled by trading ahead of the material nonpublic information contained in the Stolen Releases.

23. It was further part of the conspiracy that the Traders and others sent the Hackers a portion of the proceeds from their profitable trading using, among other methods, several shell companies.

24. It was further part of the conspiracy that using the means and methods described above, the conspiracy generated in excess of approximately \$30 million in illicit trading profits.

In violation of Title 18, United States Code, Section 1349.

Count Two
**(Conspiracy to Commit Fraud and Related
Activity in Connection with Computers)**

25. The allegations contained in paragraphs 1 through 15 of this Information are realleged and incorporated as though fully set forth in this paragraph.

26. From in or about February 2010 through in or about November 2014, in the District of New Jersey and elsewhere, defendant

VADYM IERMOLOVYCH

did knowingly and intentionally conspire and agree with others to, by means of interstate communications, intentionally access protected computers in interstate commerce without authorization, and exceed authorized access, and thereby obtain information from those computers for the purpose of commercial advantage and private financial gain, contrary to Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B)(i), and (c)(2)(B)(iii).

Object of the Conspiracy

27. It was the object of the conspiracy for defendant IERMOLOVYCH and others to enrich themselves by: (a) gaining unauthorized access to the computer networks of the Victim Newswires, including by misrepresenting their identities in order to gain access to information that was otherwise not available to them; (b) stealing confidential business information from those networks, including press releases containing material nonpublic information concerning publicly traded companies – namely the Stolen Releases; (c) trading

ahead of the material nonpublic information contained in the Stolen Releases; and (d) sharing in the proceeds of the profitable illegal trading.

Manner and Means of the Conspiracy

28. It was part of the conspiracy that defendant IERMOLOVYCH and others employed the manner and means set forth in paragraphs 19 through 24 of this Information.

Overt Acts

29. In furtherance of the conspiracy and to effect the unlawful objects thereof, defendant IERMOLOVYCH and others committed and caused to be committed the following overt acts, among others, in the District of New Jersey and elsewhere:

- a. From in or about July 2010 through in or about January 2011, the Hackers hacked into the computer networks of PRN.
- b. From in or about July 2011 through in or about March 2012, the Hackers hacked into the computer networks of PRN.
- c. On or about March 26, 2012, co-conspirator Ieremenko sent co-conspirator Turchynov a link to malware placed within the networks of Business Wire.
- d. Between on or about March 26, 2012 and on or about June 5, 2012, on approximately 39 occasions, co-conspirator Turchynov accessed malware that had been installed on Business Wire's networks.

e. Between on or about April 24, 2012 and on or about July 20, 2012, co-conspirator Turchynov sent SQL Injection Attack commands into the networks of Marketwired on at least 390 occasions.

f. From in or about January 2013 through in or about March 2013, the Hackers, including defendant IERMOLOVYCH, hacked into the computer networks of PRN.

In violation of Title 18, United States Code, Section 371.

Count Three
(Aggravated Identity Theft)

30. The allegations contained in paragraphs 1 through 15 of this Information are realleged and incorporated as though fully set forth in this paragraph.

31. On or about February 27, 2013, in the District of New Jersey and elsewhere, defendant

VADYM IERMOLOVYCH

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another individual, namely, a username and password of Employee #1, during and in relation to a felony violation of a provision enumerated in Title 18, United States Code, Section 1028A(c), that is, conspiracy to commit fraud and related activity in connection with computers as described in Count Two of this Information.

In violation of Title 18, United States Code, Section 1028A(a)(1), and Title 18, United States Code, Section 2.

FORFEITURE ALLEGATION AS TO COUNT ONE

1. As a result of committing the offense of conspiracy to commit wire fraud, contrary to 18 U.S.C. § 1343, in violation of 18 U.S.C. § 1349, as charged in Count One of this Information, the defendant VADYM IERMOLOVYCH shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of the said conspiracy offense, and all property traceable to such property.

FORFEITURE ALLEGATION AS TO COUNT TWO

2. As a result of committing the offenses alleged in Count Two of this Information, the defendant VADYM IERMOLOVYCH shall forfeit to the United States

a. pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of the offense charged in Count Two; and

b. pursuant to 18 U.S.C. § 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of the offense charged in Count Two.


SUBSTITUTE ASSETS PROVISION
(Applicable to All Forfeiture Allegations)

3. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

- b. has been transferred or sold to, or deposited with a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

the United States shall be entitled, pursuant to 21 U.S.C. § 853(p) (as incorporated by 28 U.S.C. § 2461(c), 18 U.S.C. § 1030(i), and 18 U.S.C. § 982(b)), to forfeiture of any other property of the defendant up to the value of the above-described forfeitable property.



PAUL J. FISHMAN
United States Attorney

CASE NUMBER:

**United States District Court
District of New Jersey**

UNITED STATES OF AMERICA

v.

VADYM IERMOLOVYCH

a/k/a "Vadim Ermolovich,"

a/k/a "Dima Ermolovich,"

a/k/a "Dim,"

a/k/a "Dima,"

a/k/a "Dingos777,"

a/k/a "Vaer,"

a/k/a "Nadal,"

a/k/a "PriestTF," and

a/k/a "Kamazik"

INFORMATION FOR

18 U.S.C. § 1349, 18 U.S.C. § 371,
and 18 U.S.C. § 1028A(a)(1)

PAUL J. FISHMAN

UNITED STATES ATTORNEY

NEWARK, NEW JERSEY

DANIEL SHAPIRO

ASSISTANT U.S. ATTORNEY

NEWARK, NEW JERSEY

(973) 353-6087
