

A. Natürliche Personen

▼ **M3**

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
1.	GAO Qiang	Geburtsdatum: 4. Oktober 1983 Geburtsort: Provinz Shandong, China Anschrift: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Staatsangehörigkeit: chinesisch Geschlecht: männlich	Gao Qiang ist an „Operation Cloud Hopper“ beteiligt, einer Reihe von Cyberangriffen mit erheblichen Auswirkungen, die von außerhalb der Union verübt werden und eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, und von Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten. Mit „Operation Cloud Hopper“ wurden Informationssysteme multinationaler Unternehmen auf sechs Kontinenten angegriffen, darunter Unternehmen mit Sitz in der Union, und unbefugt auf sensible Geschäftsdaten zugegriffen, was zu erheblichen wirtschaftlichen Verlusten geführt hat. „Operation Cloud Hopper“ wurde von dem als „APT10“ („Advanced Persistent Threat 10“) (alias „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ und „Potassium“) bekannten Täter verübt. Gao Qiang kann mit APT10 in Verbindung gebracht werden, auch aufgrund seiner Verbindungen zur Führungs- und Kontrollinfrastruktur von APT10. Überdies ist er bei Huaying Haitai beschäftigt, einer Organisation, die benannt wurde, weil sie „Operation Cloud Hopper“ unterstützt und ermöglicht. Er unterhält Verbindungen zu Zhang Shilong, der auch im Zusammenhang mit „Operation Cloud Hopper“ benannt wurde. Gao Qiang steht somit sowohl mit Huaying Haitai als auch mit Zhang Shilong in Verbindung.	30.7.2020
2.	ZHANG Shilong	Geburtsdatum: 10. September 1981 Geburtsort: China Anschrift: Hedong, Yuyang Road No 121, Tianjin, China Staatsangehörigkeit: chinesisch Geschlecht: männlich	Zhang Shilong ist an „Operation Cloud Hopper“ beteiligt, einer Reihe von Cyberangriffen mit erheblichen Auswirkungen, die von außerhalb der Union verübt werden und eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, und von Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten. Mit „Operation Cloud Hopper“ wurden Informationssysteme multinationaler Unternehmen auf sechs Kontinenten angegriffen, darunter Unternehmen mit Sitz in der Union, und unbefugt auf sensible Geschäftsdaten zugegriffen, was zu erheblichen wirtschaftlichen Verlusten geführt hat. „Operation Cloud Hopper“ wurde von dem als „APT10“ („Advanced Persistent Threat 10“) (alias „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ und „Potassium“) bekannten Täter verübt. Zhang Shilong kann mit APT10 in Verbindung gebracht werden, auch über die Schadsoftware, die er im Zusammenhang mit den Cyberangriffen von APT10 entwickelt und getestet hat. Überdies ist er bei Huaying Haitai beschäftigt, einer Organisation, die benannt wurde, weil sie „Operation Cloud Hopper“ unterstützt und ermöglicht. Er unterhält Verbindungen zu Gao Qiang, der auch im Zusammenhang mit „Operation Cloud Hopper“ benannt wurde. Zhang Shilong steht somit sowohl mit Huaying Haitai als auch mit Gao Qiang in Verbindung.	30.7.2020

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
3.	Alexey Valeryevich MININ	<p>Алексей Валерьевич МИНИН</p> <p>Geburtsdatum: 27.5.1972</p> <p>Geburtsort: Oblast Perm, Russische SFSR (jetzt Russische Föderation)</p> <p>Reisepass-Nr.: 120017582</p> <p>ausgestellt vom Außenministerium der Russischen Föderation</p> <p>gültig vom 17.4.2017 bis zum 17.4.2022</p> <p>Ort: Moskau, Russische Föderation</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>Alexey Minin hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten teilgenommen.</p> <p>Als für ‚human intelligence‘ (Aufklärung mit menschlichen Quellen) zuständiger Mitarbeiter der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) gehörte Alexey Minin einem Team von vier Beamten des russischen Militärsgeheimdienstes an, die im April 2018 versuchten, sich unbefugt Zugang zum WiFi-Netz der OVCW in Den Haag (Niederlande) zu verschaffen. Der versuchte Cyberangriff hatte zum Ziel, in das WiFi-Netz der OVCW einzudringen, was bei Erfolg die Sicherheit des Netzes und die laufenden Untersuchungen der OVCW gefährdet hätte. Der niederländische militärische Nachrichten- und Sicherheitsdienst (Militaire Inlichtingen- en Veiligheidsdienst) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schweren Schaden bewahrt.</p> <p>Eine Grand Jury des Western District of Pennsylvania (Vereinigte Staaten von Amerika) hat Alexey Minin als Beamter der Hauptdirektion des russischen Militärsgeheimdienstes (GRU) wegen Computerhackings, Telekommunikationsbetrugs, schweren Identitätsdiebstahls und Geldwäsche angeklagt.</p>	30.7.2020

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
4.	Aleksei Sergeyvich MORENETS	<p>Алексей Сергеевич МОРЕНЕЦ</p> <p>Geburtsdatum: 31.7.1977</p> <p>Geburtsort: Oblast Murmansk, Russische SFSR (jetzt Russische Föderation)</p> <p>Reisepass-Nr.: 100135556</p> <p>ausgestellt vom Außenministerium der Russischen Föderation</p> <p>gültig vom 17.4.2017 bis zum 17.4.2022</p> <p>Ort: Moskau, Russische Föderation</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>Aleksei Morenets hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten teilgenommen.</p> <p>Als Cyber-Operator der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) gehörte Aleksei Morenets einem Team von vier Beamten des russischen Militärgeheimdienstes an, die im April 2018 versuchten, sich unbefugt Zugang zum WiFi-Netz der OVCW in Den Haag (Niederlande) zu verschaffen. Der versuchte Cyberangriff hatte zum Ziel, in das WiFi-Netz der OVCW einzudringen, was bei Erfolg die Sicherheit des Netzes und die laufenden Untersuchungen der OVCW gefährdet hätte. Der niederländische militärische Nachrichten- und Sicherheitsdienst (Militaire Inlichtingen- en Veiligheidsdienst) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schweren Schaden bewahrt.</p> <p>Eine Grand Jury des Western District of Pennsylvania (Vereinigte Staaten von Amerika) hat Aleksei Morenets, der der Militäreinheit 26165 zugewiesen ist, wegen Computerhackings, Telekommunikationsbetrugs, schweren Identitätsdiebstahls und Geldwäsche angeklagt.</p>	30.7.2020

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
5.	Evgenii Mikhaylovich SEREBRIAKOV	<p>Евгений Михайлович СЕРЕБРЯКОВ</p> <p>Geburtsdatum: 26.7.1981</p> <p>Geburtsort: Kursk, Russische SFSR (jetzt Russische Föderation)</p> <p>Reisepass-Nr.: 100135555</p> <p>ausgestellt vom Außenministerium der Russischen Föderation</p> <p>gültig vom 17.4.2017 bis zum 17.4.2022</p> <p>Ort: Moskau, Russische Föderation</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>Evgenii Serebriakov hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten teilgenommen.</p> <p>Als Cyber-Operator der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) gehörte Evgenii Serebriakov einem Team von vier Beamten des russischen Militärgeheimdienstes an, die im April 2018 versuchten, sich unbefugt Zugang zum WiFi-Netz der OVCW in Den Haag (Niederlande) zu verschaffen. Der versuchte Cyberangriff hatte zum Ziel, in das WiFi-Netz der OVCW einzudringen, was bei Erfolg die Sicherheit des Netzes und die laufenden Untersuchungen der OVCW gefährdet hätte. Der niederländische militärische Nachrichten- und Sicherheitsdienst (Militaire Inlichtingen- en Veiligheidsdienst) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schweren Schaden bewahrt.</p> <p>Seit Frühjahr 2022 ist Evgenii Serebriakov Anführer von ‚Sandworm‘ (alias ‚Sandworm Team‘, ‚BlackEnergy Group‘, ‚Voodoo Bear‘, ‚Quedagh‘, ‚Olympic Destroyer‘ und ‚Telebots‘), einer Täter- und Hackergruppe, die mit der Einheit 74455 der Hauptdirektion des russischen Militärgeheimdienstes in Verbindung steht. Sandworm hat im Zuge des Angriffskriegs Russlands gegen die Ukraine Cyberangriffe auf die Ukraine, einschließlich auf ukrainische Regierungsstellen, verübt.</p>	30.7.2020

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
6.	Oleg Mikhaylovich SOTNIKOV	<p>Олег Михайлович СОТНИКОВ</p> <p>Geburtsdatum: 24.8.1972</p> <p>Geburtsort: Uljanowsk, Russische SFSR (jetzt Russische Föderation)</p> <p>Reisepass-Nr.: 120018866</p> <p>ausgestellt vom Außenministerium der Russischen Föderation</p> <p>gültig vom 17.4.2017 bis zum 17.4.2022</p> <p>Ort: Moskau, Russische Föderation</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>Oleg Sotnikov hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten teilgenommen.</p> <p>Als für ‚human intelligence‘ (Aufklärung mit menschlichen Quellen) zuständiger Mitarbeiter der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) gehörte Oleg Sotnikov einem Team von vier Beamten des russischen Militärgeheimdienstes an, die im April 2018 versuchten, sich unbefugt Zugang zum WiFi-Netz der OVCW in Den Haag (Niederlande) zu verschaffen. Der versuchte Cyberangriff hatte zum Ziel, in das WiFi-Netz der OVCW einzudringen, was bei Erfolg die Sicherheit des Netzes und die laufenden Untersuchungen der OVCW gefährdet hätte. Der niederländische militärische Nachrichten- und Sicherheitsdienst (Militaire Inlichtingen- en Veiligheidsdienst) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schweren Schaden bewahrt.</p> <p>Eine Grand Jury des Western District of Pennsylvania hat Oleg Sotnikov als Beamter der Hauptdirektion des russischen Militärgeheimdienstes (GRU) wegen Computerhackings, Telekommunikationsbetrugs, schweren Identitätsdiebstahls und Geldwäsche angeklagt.</p>	30.7.2020

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
7.	Dmitry Sergeyevich BADIN	<p>Дмитрий Сергеевич БАДИН</p> <p>Geburtsdatum: 15.11.1990</p> <p>Geburtsort: Kursk, Russische SFSR (jetzt Russische Föderation)</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>Dmitry Badin war an einem Cyberangriff mit erheblichen Auswirkungen gegen den Deutschen Bundestag sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten beteiligt.</p> <p>Als Militärgeheimdienstbeamter des 85. Hauptzentrums für Spezialdienste (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) war Dmitry Badin Teil eines Teams von Beamten des russischen Militärgeheimdienstes, die im April und Mai 2015 einen Cyberangriff gegen den Deutschen Bundestag durchführten. Dieser Cyberangriff zielte auf das Informationssystem des Parlaments ab und beeinträchtigte dessen Betrieb für mehrere Tage. Es wurde eine beträchtliche Menge an Daten gestohlen, und die E-Mail-Konten mehrerer MdB sowie der ehemaligen Bundeskanzlerin Angela Merkel waren betroffen.</p> <p>Eine Grand Jury des Western District of Pennsylvania (Vereinigte Staaten von Amerika) hat Dmitry Badin, der der Militäreinheit 26165 zugewiesen ist, wegen Computerhackings, Telekommunikationsbetrugs, schweren Identitätsdiebstahls und Geldwäsche angeklagt.</p>	22.10.2020

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Geburtsdatum: 21.2.1961 Staatsangehörigkeit: russisch Geschlecht: männlich	<p>Igor Kostyukov ist derzeit Leiter der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU), wo er zuvor als Erster Stellvertretender Leiter tätig war. Eine der seiner Befehlsgewalt unterstehenden Einheiten ist das 85. Hauptzentrum für Spezialdienste (GTsST), (alias ‚Militäreinheit 26165‘, ‚APT28‘, ‚Fancy Bear‘, ‚Sofacy Group‘, ‚Pawn Storm‘ und ‚Strontium‘).</p> <p>In dieser Eigenschaft ist Igor Kostyukov verantwortlich für vom GTsST durchgeführte Cyberangriffe, einschließlich derjenigen mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p> <p>Militärgeheimdienstbeamte des GTsST waren insbesondere beteiligt am Cyberangriff gegen den Deutschen Bundestag im April und Mai 2015, und an dem versuchten Cyberangriff vom April 2018 in den Niederlanden mit dem Ziel, sich unbefugt Zugang zum WiFi-Netz der Organisation für das Verbot chemischer Waffen (OVCW) zu verschaffen.</p> <p>Der Cyberangriff gegen den Deutschen Bundestag zielte auf das Informationssystem des Parlaments ab und beeinträchtigte dessen Betrieb für mehrere Tage. Es wurde eine beträchtliche Menge an Daten gestohlen, und die E-Mail-Konten mehrerer MdB sowie der ehemaligen Bundeskanzlerin Angela Merkel waren betroffen.</p>	22.10.2020

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
9.	Ruslan Aleksandrovich PERETYATKO	<p>Руслан Александрович ПЕРЕТЯТКО</p> <p>Geburtsdatum: 3.8.1985</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>Ruslan PERETYATKO war an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p> <p>Ruslan PERETYATKO gehört der ‚Callisto‘-Gruppe an, einer Gruppe von Beamten des russischen Geheimdienstes, die Cyberoperationen gegen Mitgliedstaaten der EU und Drittstaaten durchführt.</p> <p>Die ‚Callisto‘-Gruppe (alias ‚Seaborgium‘, ‚Star Blizzard‘, ‚ColdRiver‘, ‚TA446‘) hat mehrjährige Phishing-Kampagnen gestartet, um Kontozugangsdaten und Daten zu stehlen. Darüber hinaus zeichnet die ‚Callisto‘-Gruppe für Kampagnen verantwortlich, die sich gegen Einzelpersonen und kritische staatliche Funktionen, auch in den Bereichen Verteidigung und Außenbeziehungen, richten.</p> <p>Deshalb ist Ruslan PERETYATKO an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p>	24.6.2024
10.	Andrey Stanislavovich KORINETS	<p>Андрей Станиславович КОРИНЕЦ</p> <p>Geburtsdatum: 18.5.1987</p> <p>Geburtsort: Stadt Syktyvkar, Russland</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>Andrey Stanislavovich KORINETS war an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p> <p>Andrey Stanislavovich KORINETS ist Offizier des ‚Center 18‘ des Inlandsgeheimdienstes der Russischen Föderation. Andrey Stanislavovich KORINETS gehört der ‚Callisto-Gruppe‘ an, einer Gruppe von Beamten des russischen Geheimdienstes, die Cyberoperationen gegen Mitgliedstaaten der EU und Drittstaaten durchführt.</p> <p>Die ‚Callisto‘-Gruppe (alias ‚Seaborgium‘, ‚Star Blizzard‘, ‚ColdRiver‘, ‚TA446‘) hat mehrjährige Phishing-Kampagnen gestartet, um Kontozugangsdaten und Daten zu stehlen. Darüber hinaus zeichnet die ‚Callisto‘-Gruppe für Kampagnen verantwortlich, die sich gegen Einzelpersonen und kritische staatliche Funktionen, auch in den Bereichen Verteidigung und Außenbeziehungen, richten.</p> <p>Deshalb ist Andrey Stanislavovich KORINETS an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p>	24.6.2024

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
11.	Oleksandr SKLIANKO	Александр СКЛЯНКО (russische Schreibweise) Олександр СКЛЯНКО (ukrainische Schreibweise) Geburtsdatum: 5.8.1973 Reisepass: EC 867868, ausgestellt am 27.11.1998 (Ukraine) Geschlecht: männlich	Oleksandr SKLIANKO war an Cyberangriffen mit erheblichen Auswirkungen, die gegen Mitgliedstaaten der EU gerichtet waren, sowie an Cyberangriffen mit erheblichen Auswirkungen, die gegen Drittstaaten gerichtet waren, beteiligt. Oleksandr SKLIANKO gehört der ‚Armageddon‘-Hackergruppe an, die vom Inlandsgeheimdienst der Russischen Föderation unterstützt wird und verschiedene Cyberangriffe mit erheblichen Auswirkungen durchgeführt hat, die gegen die Regierung der Ukraine und gegen Mitgliedstaaten der EU und deren Regierungsbeamte gerichtet waren, unter anderem mittels Phishing-E-Mails und Schadsoftware-Kampagnen. Deshalb ist Oleksandr SKLIANKO an Cyberangriffen mit erheblichen Auswirkungen, die gegen Drittstaaten gerichtet sind, sowie an Cyberangriffen mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, beteiligt.	24.6.2024
12.	Mykola CHERNYKH	Николай ЧЕРНЫХ (russische Schreibweise) Микола ЧЕРНИХ (ukrainische Schreibweise) Geburtsdatum: 12.10.1978 Reisepass: EC 922162, ausgestellt am 20.1.1999 (Ukraine) Geschlecht: männlich	Mykola CHERNYKH war an Cyberangriffen mit erheblichen Auswirkungen, die gegen Mitgliedstaaten der EU gerichtet waren, sowie an Cyberangriffen mit erheblichen Auswirkungen, die gegen Drittstaaten gerichtet waren, beteiligt. Mykola CHERNYKH gehört der ‚Armageddon‘-Hackergruppe an, die vom Inlandsgeheimdienst der Russischen Föderation unterstützt wird und verschiedene Cyberangriffe mit erheblichen Auswirkungen durchgeführt hat, die gegen die Regierung der Ukraine und gegen Mitgliedstaaten der EU und deren Regierungsbeamte gerichtet waren, unter anderem mittels Phishing-E-Mails und Schadsoftware-Kampagnen. Als ehemaliger Mitarbeiter des Sicherheitsdienstes der Ukraine ist er in der Ukraine des Verrats und des unberechtigten Eingriffs in den Betrieb elektronischer Rechner und automatisierter Systeme angeklagt. Deshalb ist Mykola CHERNYKH an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.	24.6.2024

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
13.	Mikhail Mikhailovich TSAREV	<p>Михаил Михайлович ЦАРЕВ</p> <p>Geburtsdatum: 20.4.1989</p> <p>Geburtsort: Serpukhov, Russische Föderation</p> <p>Staatsangehörigkeit: russisch</p> <p>Anschrift: Serpukhov</p> <p>Geschlecht: männlich</p>	<p>Mikhail Mikhailovich TSAREV war an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Mitgliedstaaten der EU darstellen.</p> <p>Mikhail Mikhailovich TSAREV, auch bekannt unter den Online-Spitznamen ‚Mango‘, ‚Alexander Grachev‘, ‚Super Misha‘, ‚Ivanov Mixail‘, ‚Misha Krutysha‘ und ‚Nikita Andreevich Tsarev‘, ist ein wichtiger Akteur in der Einsetzung der Schadsoftware ‚Conti‘ und ‚Trickbot‘ und ist an der Russland-basierten Bedrohungsgruppe ‚Wizard Spider‘ beteiligt.</p> <p>Die Schadsoftware ‚Conti‘ und ‚Trickbot‘ wurde von ‚Wizard Spider‘ geschaffen und entwickelt wurde. Die Gruppe ‚Wizard Spider‘ hat in verschiedenen Branchen, darunter wesentliche Dienstleistungsbereiche wie die Gesundheitsversorgung und das Bankwesen, Ransomware-Kampagnen durchgeführt. Die Gruppe hat weltweit Computer infiziert und ihre Schadsoftware in eine hochmodulare Schadsoftware-Reihe entwickelt. Von der Gruppe ‚Wizard Spider‘ durchgeführte Kampagnen, bei denen Schadsoftware wie ‚Conti‘, ‚Ryuk‘ und ‚TrickBot‘, eingesetzt wird, sind für erhebliche wirtschaftliche Schäden in der Europäischen Union verantwortlich.</p> <p>Deshalb ist Mikhail Mikhailovich TSAREV an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p>	24.6.2024

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
14.	Maksim Sergeevich GALOCHKIN	<p>Максим Сергеевич ГАЛОЧКИН</p> <p>Geburtsdatum: 19.5.1982</p> <p>Geburtsort: Abakan, Russische Föderation</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>Maksim Galochkin hat bei Cyberangriffen mit erheblichen Auswirkungen mitgewirkt, die eine externe Bedrohung für die Mitgliedstaaten der EU darstellen.</p> <p>Maksim Galochkin ist auch bekannt unter den Online-Spitznamen ‚Benalen‘, ‚Bentley‘, ‚Volhvb‘, ‚volhvb‘, ‚manuel‘, ‚Max17‘ und ‚Crypt‘. Galochkin ist ein wichtiger Akteur in der Einsetzung der Schadsoftware ‚TrickBot‘ und ‚Conti‘ und ist an der Russland-basierten Bedrohungsgruppe ‚Wizard Spider‘ beteiligt. Er hat ein Team von Testern geleitet, das mit für die Entwicklung, Überwachung und Durchführung von Tests für die von ‚Wizard Spider‘ geschaffene und eingesetzte TrickBot-Schadsoftware verantwortlich war.</p> <p>‚Wizard Spider‘ hat in verschiedenen Branchen, darunter wesentliche Dienstleistungsbereiche wie die Gesundheitsversorgung und das Bankwesen, Ransomware-Kampagnen durchgeführt. Die Gruppe hat weltweit Computer infiziert und ihre Schadsoftware in eine hochmodulare Schadsoftware-Reihe entwickelt. Von der Gruppe ‚Wizard Spider‘ durchgeführte Kampagnen, bei denen Schadsoftware wie ‚Conti‘, ‚Ryuk‘ und ‚TrickBot‘, eingesetzt wird, sind für erhebliche wirtschaftliche Schäden in der Europäischen Union verantwortlich.</p> <p>Deshalb ist Maksim Galochkin an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p>	24.6.2024