Shift Happens

Wie sich Cybercrime und IR in fünf Jahren verändert haben

Leonard Rapp
Security Engineer DFIR
CSIRT
G DATA Advanced Analytics GmbH

Jasper Bongertz
Principal Network Security Specialist
Head of CSIRT
G DATA Advanced Analytics GmbH

G DATA
advanced analytics

G DATA
advanced analytics

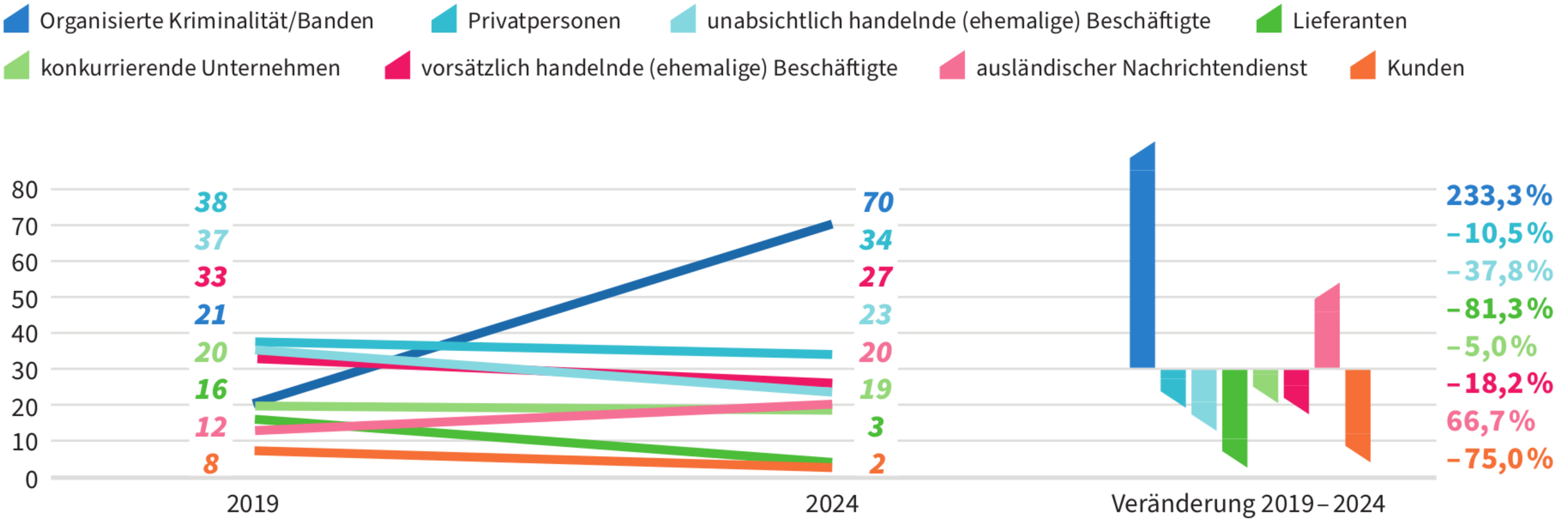
A long time ago

in a university hospital far, far away...

Gut organisiert

IT-Angriffe auf Unternehmen nach Täterkreis; Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr, die in den vergangenen zwölf Monaten von Diebstahl, Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2024: n=812; 2019: n=801); Deutschland; in Prozent*

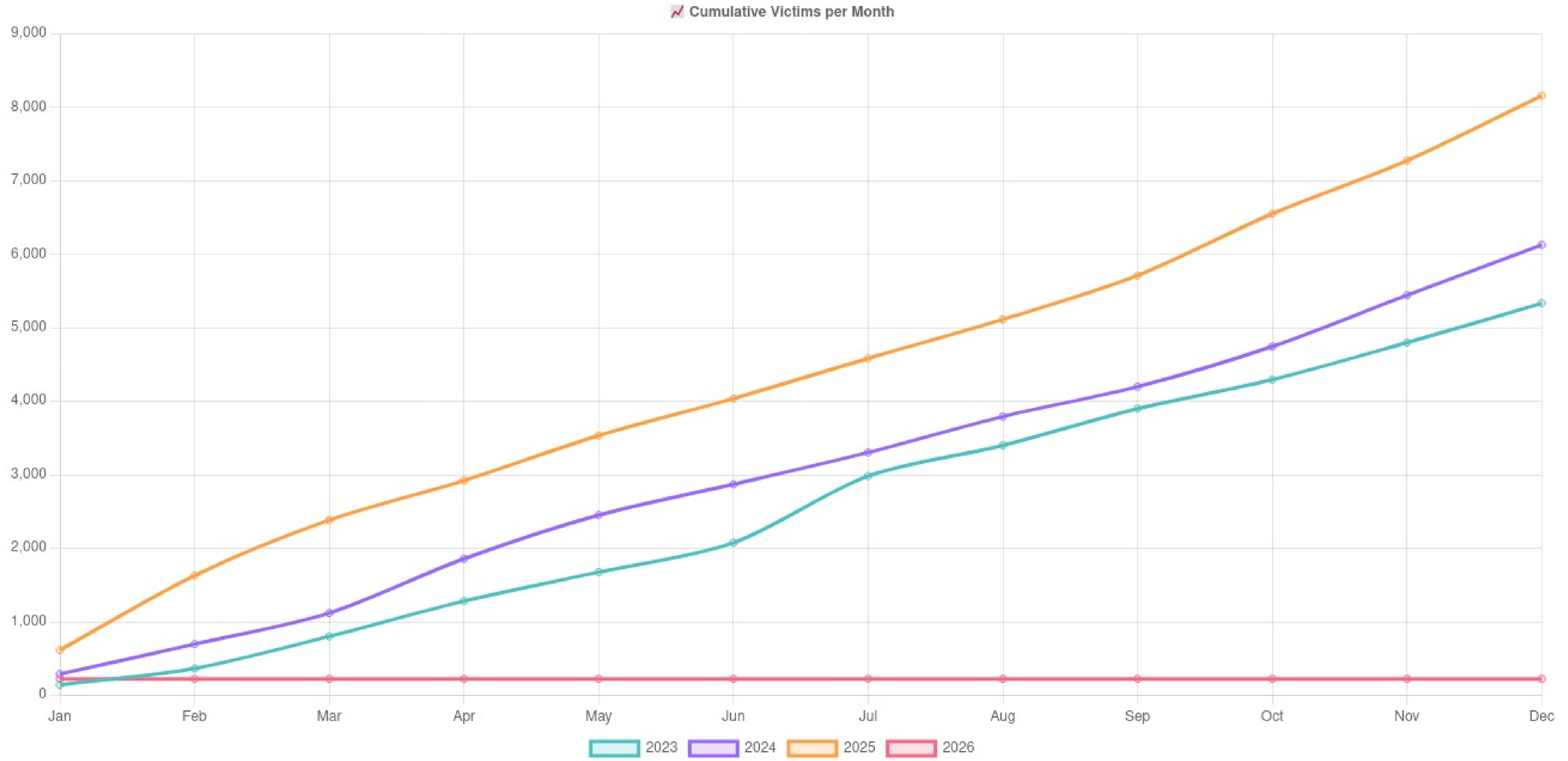
Von welchem Täterkreis gingen die Handlungen in den vergangenen zwölf Monaten aus?



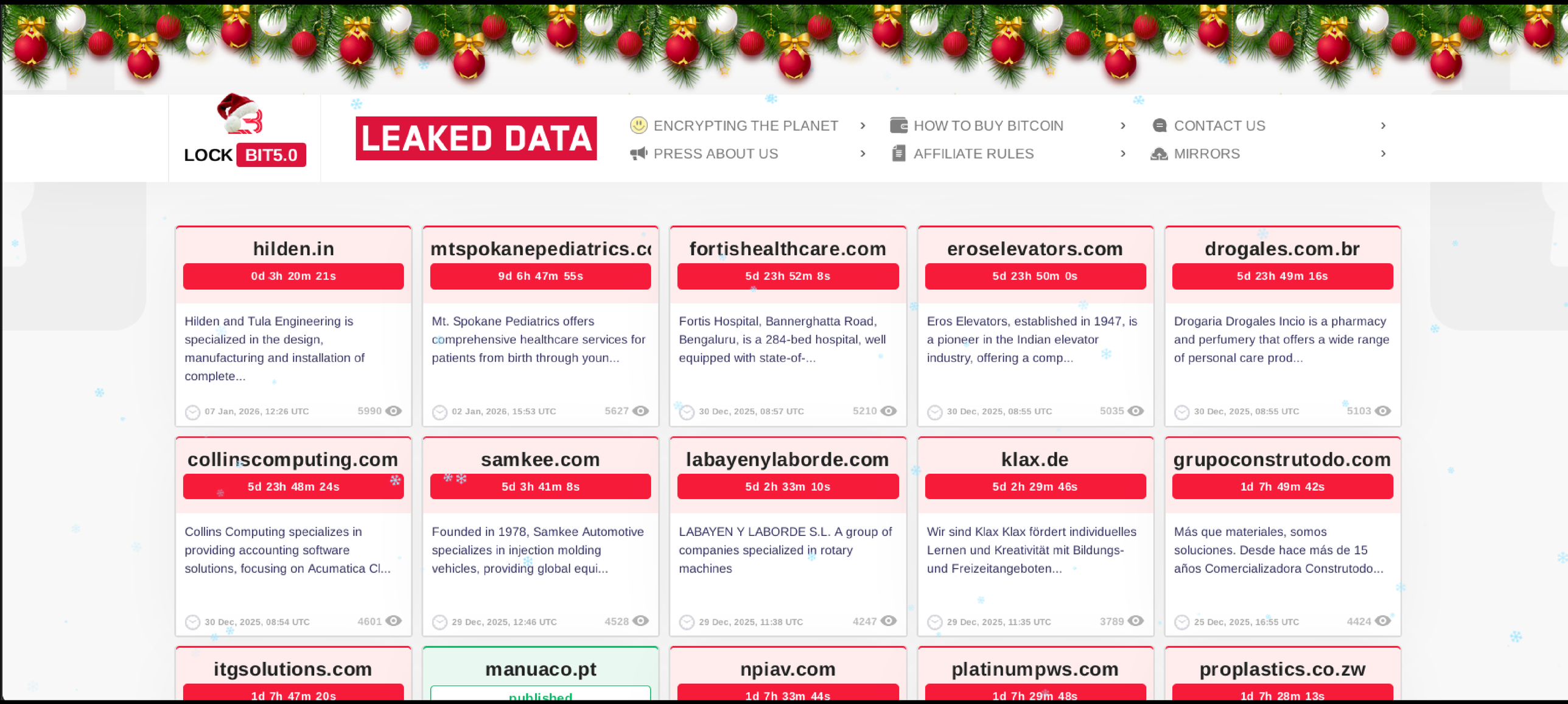
*Mehrfachnennungen möglich. Quelle: Bitkom

Quelle: Cybersicherheit in Zahlen 2025/2026

Cumulative Victims per Month (2023–2026)



Quelle: https://www.ransomware.live/stats



G DATA advanced analytics

LOCK BIT5.0

LEAKED DATA

ENCRYPTING THE PLANET › | HOW TO BUY BITCOIN › | CONTACT US ›

PRESS ABOUT US › | AFFILIATE RULES › | MIRRORS ›

AFFILIATE RULES

The immortal oldest Ransomware affiliate program LockBit is excited to welcome you.

We have been working since September 3, 2019 and we are not going to stop no matter how much the intelligence services around the world want us to stop.

Fachkräftemangel

Command I am trying to run a cmd file that calls a PowerShell script from cmd.exe, but I am getting this error:

Command Management_Install.ps1 cannot be loaded because the execution of scripts is disabled on this system.

Command I ran this command:

Command Set-ExecutionPolicy -ExecutionPolicy Unrestricted

Мануал по работе с сетями

от Bassterlord (FishEye)

Если только на нескольких машинах значит только права локальных администраторов и стоит искать другие учетные записи.

Если у нас нет открытых паролей а только хеши которые не вышло расшифровать мы рассмотрим уязвимости входа по хешам в разделе PASS THE HASH атак.

Если в открытом компьютере с красным диском C$ нет порта 3389 можно использовать тулзу psexec которую мы рассмотрим в отдельном разделе.

Если мы пробили через уязвимость сервер - определить его можно по следующим параметрам и сравнив айпи сессий:

Либо по имени хоста в котором присутствует DC

Например WHDC.domain.local (значения могут быть любыми нам важно узнать именно DC)

Тогда можно

В сессии сервиса выполнить команды

shell

net group

net group "Domain Admins" /domain

Это поможет узнать нам учетные записи администраторов домена и соответственно не отвлекается на обычных юзеров и их аккаунты.

Нам ведь важен уровень «БОГ» да?)

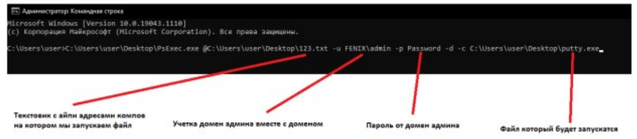
В этом разделе мы рассмотрим тулзу Psexec и чем она будет полезна на практике.

Первым делом она поможет нам запустить любой файл на всех тачках к которым у нас есть доступ.

Предположим у нас есть exe файл который нам нужно запустить

Открываем CMD перетаскиваем туда psexec.exe

и далее пишем следующее



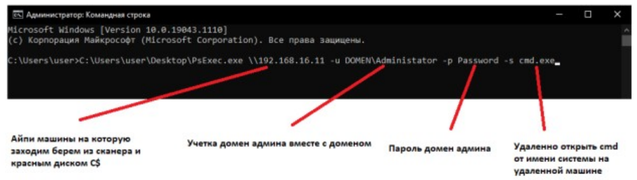
Если вы удалили все ав добавили исключения и сделали все как нужно данный exe будет запущен на всех компах.

Если вам нужно запустить файл от имени системы добавляем к параметрам -s -d -c файл.exe

Через Psexec можно получить и снять креды с удаленных компов если на них нет 3389 порта но учетка у нас есть.

Через сканер открываем папку C$ закидываем туда pesecdump.exe

и procdump.exe



G DATA advanced analytics

Strafverfolgungsbehörden

G DATA
advanced analytics

THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

7

NCA National Crime Agency
South West ROCU
Metropolitan Police
EUROPOL
POLITIE
Bundeskriminalamt
Kanton Zürich
Gendarmerie nationale
SH Schleswig-Holstein Landeskriminalamt
POLIISI Keskusrikospoliisi

SEIZED LOCKBIT 3.0

LEAKED DATA

THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

NCA National Crime Agency

EUROPOL

Press Releases

PUBLISHED

Updated: 01 Feb, 2024, 04:12 UTC 3947

LB Backend Leaks

PUBLISHED

NCA National Crime Agency

Updated: 31 Jan, 2024, 01:44 UTC 1182

Lockbitsupp

PUBLISHED

You've Been Banned From LOCKBIT 3.0

Updated: 31 Jan, 2024, 01:44 UTC 1182

Who is LockbitSupp?

PUBLISHED

The $10m question

Updated: 01 Feb, 2024, 04:12 UTC 31337

Lockbit Decryption Keys

PUBLISHED

LOCKBIT 3.0

Law Enforcement may be able to assist you to decrypt your Lockbit encrypted

Updated: 01 Feb, 2024, 04:12 UTC 3947

NEW

Rewards for Reporting

PUBLISHED

Collect up to $15,000,000 for providing information leading to the arrest of LockBit Administrators and Affiliates

Updated: 31 Jan, 2024, 01:44 UTC 1182

US Indictments

PUBLISHED

FBI Investigation Leads to a Total of 5 LockBit Affiliates Charged By the Department of Justice. Two of Those Indictments Released Today.

Updated: 31 Jan, 2024, 01:44 UTC 1182

Sanctions

PUBLISHED

United States Sanctions for Threat Actors Engaged in Significant Malicious Cyber Related Activity

Updated: 31 Jan, 2024, 01:44 UTC 1182

NEW

FR arrest warrants

PUBLISHED

JUNALCO

French Gendarmerie Investigation leads to a total of 3 Lockbit affiliates and related actors charged by the

UPDATED

Arrest in Poland

PUBLISHED

On 20/02/2024 a suspected LockBit actor was arrested in Poland on the request of French.

UPDATED

Activity in Ukraine

PUBLISHED

On 20/02/2024 a suspected LockBit actor was arrested in Ukraine on the request of France.

Report Cyber Attacks!

PUBLISHED

Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive action, it is vital that victims report attacks and

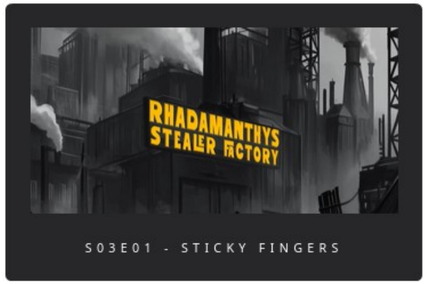
id:1 admin created_at:2022-01-31 22:20:43	id:51 Malin created_at:2022-06-25 13:02:08	id:101 Travion created_at:2022-06-25 14:31:50	id:151 Zohan created_at:2023-10-07 23:06:25
id:2 Harold created_at:2022-06-25 12:31:59	id:52 Stanton created_at:2022-06-25 13:02:33	id:102 Rupert created_at:2022-06-25 14:32:35	id:152 Weldon created_at:2023-10-21 13:54:43
id:3 Beverley created_at:2022-06-25 12:35:17	id:53 Carlo created_at:2022-06-25 13:02:55	id:103 Jeffrey created_at:2022-06-25 14:32:57	id:153 Chris created_at:2023-10-25 02:24:05
id:4 Jaye created_at:2022-06-25 12:35:40	id:54 Alston created_at:2022-06-25 13:03:35	id:104 Shepard created_at:2022-06-25 14:33:31	id:154 Reinhold created_at:2023-10-27 22:50:18
id:5 Finn created_at:2022-06-25 12:36:00	id:55 Merrick created_at:2022-06-25 13:05:38	id:105 Williams created_at:2022-06-25 14:39:14	id:155 Roscoe created_at:2023-10-28 21:32:50
id:6 Aston created_at:2022-06-25 12:36:26	id:56 Kirby created_at:2022-06-25 13:07:01	id:106 Perry created_at:2022-06-25 14:40:10	id:156 Kelton created_at:2023-12-07 20:23:56
id:7 Maximus created_at:2022-06-25 12:36:40	id:57 Keanan created_at:2022-06-25 13:07:25	id:107 Merle created_at:2022-06-25 14:42:04	id:157 Bretton created_at:2023-12-09 20:09:31
id:8 Denise created_at:2022-06-25 12:36:53	id:58 Huntley created_at:2022-06-25 13:07:43	id:108 Neely created_at:2022-06-25 14:44:09	id:158 Burdette created_at:2023-12-09 20:18:49
id:9 John created_at:2022-06-25 12:37:07	id:59 Jeffry created_at:2022-06-25 13:08:29	id:109 Oakley created_at:2022-06-25 14:44:40	id:159 Kendel created_at:2023-12-10 19:37:37
id:10 Kelsie created_at:2022-06-25 12:37:18	id:60 Everlie created_at:2022-06-25 13:12:05	id:110 Jordi created_at:2022-06-25 14:45:01	id:160 Jake created_at:2023-12-11 00:37:00
id:11 Ramsey created_at:2022-06-25 12:37:33	id:61 Alton created_at:2022-06-25 13:12:53	id:111 Gerry created_at:2022-06-25 14:45:39	id:161 Pax created_at:2023-12-11 21:52:37
id:12 Vern created_at:2022-06-25 12:37:47	id:62 Coleton created_at:2022-06-25 13:13:37	id:112 teststealergate2 created_at:2022-11-20 11:10:50	id:162 Katlin created_at:2023-12-12 10:14:24
id:13 Mayer created_at:2022-06-25 12:37:58	id:63 Claudio created_at:2022-06-25 13:14:18	id:113 teststealergate3 created_at:2022-11-20 11:11:03	id:163 Ashton created_at:2023-12-12 19:00:39
id:14 Devyn created_at:2022-06-25 12:38:10	id:64 Libby created_at:2022-06-25 13:14:25	id:114 Neel created_at:2022-12-24 12:17:58	id:164 Oswin created_at:2023-12-12 21:25:14
id:15 Burton created_at:2022-06-25 12:38:22	id:65 Hazel created_at:2022-06-25 13:14:53	id:115 Paygost created_at:2023-01-30 06:08:40	id:165 Allyson created_at:2023-12-13 13:44:27
id:16 Ardell created_at:2022-06-25 12:38:37	id:66 Dorian created_at:2022-06-25 13:15:06	id:116 Chargost created_at:2023-03-12 14:03:34	id:166 Falcon created_at:2023-12-13 14:00:52
id:17 Harley created_at:2022-06-25 12:38:49	id:67 Rigby created_at:2022-06-25 13:15:27	id:117 teststealergate4 created_at:2023-04-16 13:58:48	id:167 Corvin created_at:2023-12-14 16:10:18
id:18 Chad created_at:2022-06-25 12:39:01	id:68 Payden created_at:2022-06-25 13:15:57	id:118 teststealergate5 created_at:2023-04-20 17:03:41	id:168 Gunther created_at:2023-12-15 23:37:02
id:19 Truman created_at:2022-06-25 12:39:11	id:69 Hadley created_at:2022-06-25 13:16:14	id:119 teststealergate6 created_at:2023-04-20 17:03:59	id:169 Hillis created_at:2023-12-17 15:02:24
id:20 Ramzi created_at:2022-06-25 12:39:26	id:70 Dwayne created_at:2022-06-25 13:16:46	id:120 teststealergate1 created_at:2023-04-20 17:04:12	id:170 Davy created_at:2023-12-17 21:09:55
id:21 Harper created_at:2022-06-25 12:39:47	id:71 Dustin created_at:2022-06-25 13:17:49	id:121 Gerald created_at:2023-04-24 22:36:17	id:171 Washington created_at:2023-12-17 21:15:49
id:22 Harlow created_at:2022-06-25 12:40:04	id:72 Jody created_at:2022-06-25 13:18:08	id:122 Rimrel created_at:2023-05-02 19:24:14	id:172 Reymond created_at:2023-12-21 21:39:33
id:23 Bart created_at:2022-06-25 12:40:18	id:73 Frankie created_at:2022-06-25 13:18:39	id:123 Tezriedil created_at:2023-05-02 19:24:46	id:173 Stevenson created_at:2023-12-24 14:45:49
id:24 Kennan created_at:2022-06-25 12:40:35	id:74 Aric created_at:2022-06-25 13:19:12	id:124 Tahabo created_at:2023-05-02 19:25:11	id:174 Arron created_at:2023-12-30 19:02:54
id:25 Melville created_at:2022-06-25 12:40:48	id:75 Vinnie created_at:2022-06-25 13:19:53	id:125 Command created_at:2023-05-10 17:12:17	id:175 Braxton created_at:2023-12-30 21:52:14
id:26 Rubert created_at:2022-06-25 12:41:01	id:76 Bradly created_at:2022-06-25 13:21:08	id:126 federalvstavaiskolen created_at:2023-05-10 22:29:48	id:176 Rami created_at:2023-12-31 15:35:56
id:27 Bailey created_at:2022-06-25 12:41:12	id:77 Kurt created_at:2022-06-25 13:21:44	id:127 Deric created_at:2023-05-28 02:57:43	id:177 Dominic created_at:2024-01-05 06:54:06
id:28 Rich created_at:2022-06-25 12:41:29	id:78 Wynne created_at:2022-06-25 13:22:08	id:128 Tommy created_at:2023-06-16 17:16:15	id:178 Silvester created_at:2024-01-05 09:57:05
id:29 Leeland created_at:2022-06-25 12:41:41	id:79 Kameron created_at:2022-06-25 13:22:13	id:129 AlphaKiller created_at:2023-07-02 09:24:35	id:179 Johnatan created_at:2024-01-05 11:51:10
id:30 Brian created_at:2022-06-25 12:43:06	id:80 Godfrey created_at:2022-06-25 13:22:42	id:130 dududu created_at:2023-07-17 10:23:17	id:180 Delos created_at:2024-01-11 20:12:38
id:31 Charly created_at:2022-06-25 12:43:18	id:81 Rawley created_at:2022-06-25 13:23:57	id:131 Jordan created_at:2023-07-17 10:25:50	id:181 Hideo created_at:2024-01-12 22:19:32
id:32 Oscar created_at:2022-06-25 12:43:34	id:82 Quinnton created_at:2022-06-25 13:23:57	id:132 pentestululu created_at:2023-07-29 20:46:32	id:182 Avraham created_at:2024-01-18 18:40:20
id:33 Lyndsey created_at:2022-06-25 12:43:48	id:83 Brett created_at:2022-06-25 13:24:05	id:133 Greg created_at:2023-08-03 19:06:18	id:183 Anders created_at:2024-01-20 17:39:01
id:34 Oliver created_at:2022-06-25 12:44:00	id:84 Torey created_at:2022-06-25 13:24:51	id:134 Aver created_at:2023-08-16 03:33:18	id:184 Barrington created_at:2024-01-20 17:47:48
id:35 Sherwin created_at:2022-06-25 12:44:11	id:85 Ronal created_at:2022-06-25 13:55:03	id:135 Mymw created_at:2023-08-16 03:38:16	id:185 Takashi created_at:2024-01-20 21:44:26
id:36 JohnRembo created_at:2022-06-25 12:47:28	id:86 Dayton created_at:2022-06-25 14:00:16	id:136 Ward created_at:2023-08-22 19:15:45	id:186 Jan created_at:2024-01-21 20:14:22
id:37 Darrel created_at:2022-06-25 12:47:48	id:87 Niko created_at:2022-06-25 14:01:11	id:137 Guardian created_at:2023-08-25 18:58:25	id:187 Benicio created_at:2024-01-21 20:51:28
id:38 Tayler created_at:2022-06-25 12:48:16	id:88 Nicholas created_at:2022-06-25 14:01:34	id:138 Rodman created_at:2023-08-26 05:55:25	id:188 Valentino created_at:2024-01-22 19:16:15
id:39 Rayce created_at:2022-06-25 12:48:50	id:89 Mickey created_at:2022-06-25 14:02:22	id:139 Hutton created_at:2023-08-26 06:02:03	id:189 Daniel created_at:2024-01-22 20:15:33
id:40 Larry created_at:2022-06-25 12:50:08	id:90 Gannon created_at:2022-06-25 14:02:46	id:140 uluulu created_at:2023-09-01 12:49:46	id:190 Charler created_at:2024-01-29 16:31:53
id:41 Skylor created_at:2022-06-25 12:50:35	id:91 Beckett created_at:2022-06-25 14:03:15	id:141 Norman created_at:2023-09-01 12:50:16	id:191 Charlieson created_at:2024-01-29 22:50:24
id:42 Rufus created_at:2022-06-25 12:55:52	id:92 Clifton created_at:2022-06-25 14:19:24	id:142 Terell created_at:2023-09-05 11:36:47	id:192 Arlieerys created_at:2024-02-01 15:54:52
id:43 Ashlin created_at:2022-06-25 12:56:29	id:93 Edsel created_at:2022-06-25 14:19:43	id:143 Powerful created_at:2023-09-05 11:40:07	id:193 Charow created_at:2024-02-02 16:31:24
id:44 Perri created_at:2022-06-25 12:57:09	id:94 Emory created_at:2022-06-25 14:20:19	id:144 Billie created_at:2023-09-10 19:49:17	id:194 Sailor created_at:2024-02-05 18:14:20
id:45 Sage created_at:2022-06-25 12:59:44	id:95 Berton created_at:2022-06-25 14:20:47	id:145 Corrie created_at:2023-09-11 19:14:26	
id:46 BillieOLDDDDD created_at:2022-06-25 13:00:18	id:96 Wilford created_at:2022-06-25 14:21:13	id:146 Raleigh created_at:2023-09-15 23:54:48	
id:47 Corbin created_at:2022-06-25 13:00:37	id:97 Hayes created_at:2022-06-25 14:22:21	id:147 Marley created_at:2023-09-17 19:15:30	
id:48 Davidson created_at:2022-06-25 13:01:14	id:98 Ricardo created_at:2022-06-25 14:23:19	id:148 Darwin created_at:2023-09-20 19:51:55	
id:49 Bayard created_at:2022-06-25 13:01:30	id:99 Cooper created_at:2022-06-25 14:24:08	id:149 Russel created_at:2023-09-22 21:23:10	
id:50 Boyce created_at:2022-06-25 13:01:46	id:100 Wyman created_at:2022-06-25 14:27:06	id:150 Daron created_at:2023-09-29 20:07:44	

G DATA
advanced analytics

HOME NEWS SEASONS SUSPECTS PARTNERS CONTACT

SEASON 3

S03E02 - INTERLUDE



S03E01 - STICKY FINGERS

SEASON 2

S02E06 - YIN AND YANG

S02E05 - A GAMBLE TOO FAR?

S02E04 - CONSEQUENCES

SEASON 1

S01E09 - BONUS

S01E08 - NOT THE END

S01E07 - ODD ONE OUT

G DATA
advanced analytics

HOME NEWS SEASONS SUSPECTS PARTNERS CONTACT

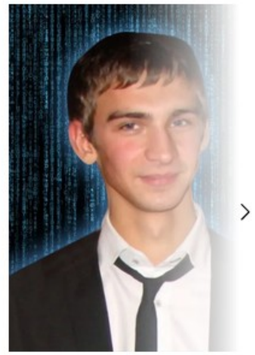
EU MOST WANTED

PROKOP, Roman Mikhailovich

SHARAFETDINOV, Iskander Rifkatovich

SEDLETSKII, Valerii

SHUPLIAKOV, Danil Alekseevich



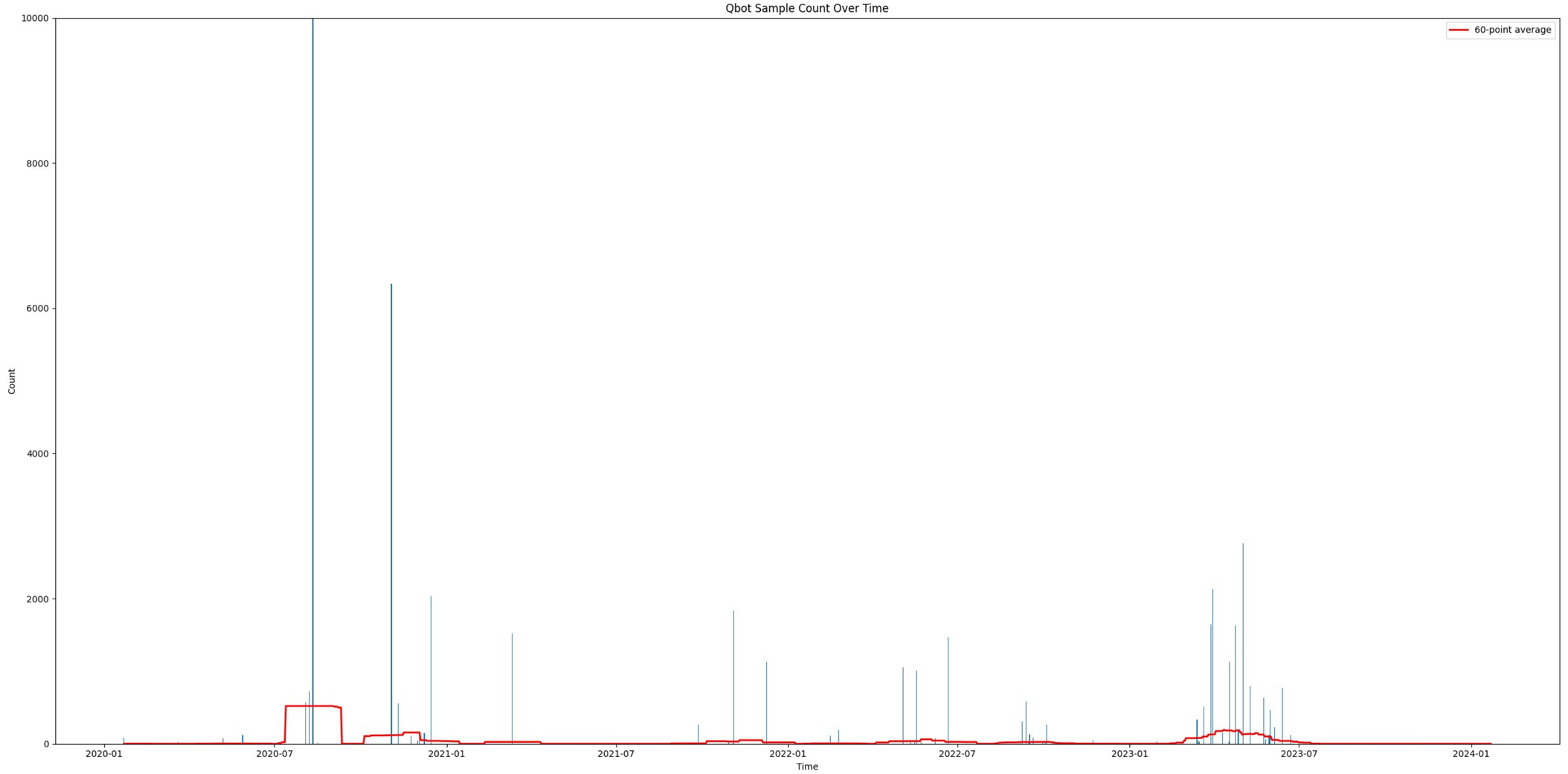
TSAREV, Mikhail Mikhailovich

DANABOT

KALINKIN, Artem

STEPANOV, Aleksandr

G DATA advanced analytics



G DATA
advanced analytics

Geopolitische Konflikte

G DATA
advanced analytics

G DATA
advanced analytics

Cyberwar eher Informationskrieg als Zerstörung

G DATA
advanced analytics

Ransomware als hybride Kriegsführung

G DATA
advanced analytics

APT

Cambodia extradites alleged scam mastermind to China after arrest

8 January 2026

Share Save

Simon Fraser
Asia editor, BBC News website

Quelle: https://www.bbc.com/news/articles/cy4q8e88n2vo

G DATA
advanced analytics

IR-Teams

G DATA
advanced analytics

Kollaborative Tools statt Einzelplatzforensik

Triage statt Full Disk Forensik

Automatisierung statt Repetition

G DATA
advanced analytics

AI ist Wechsel der Methoden,
nicht der grundlegenden Prinzipien

IT-Sicherheit ist kein technisches Problem, sondern ein organisatorisches + wirtschaftliches

G DATA
advanced analytics

Verteidigung mit bekannten Mitteln

1. VPN + 2FA
2. Netzwerksegmentierung
3. Monitoring
4. Backups
5. Notfallhandbuch

Vielen Dank für Ihre Aufmerksamkeit,
bis (hoffentlich erst) nächstes Jahr!

Notfallnummer
+49 234 9762-800

Jasper Bongertz
jasper.bongertz@gdata-adan.de
+49 172 5783558

Leonard Rapp
leonard.rapp@gdata-adan.de
+49 173 2751342