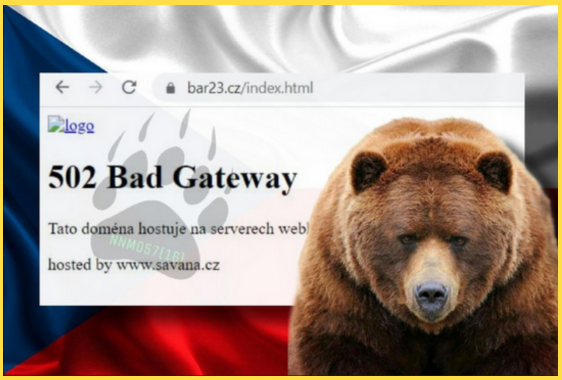
Kyberútoky proti České republice

Autoři: Abraham Tomáš, Havlík David, Šlechta Ondřej, analytici **CZECHMATE CZ s.r.o.**

Česká republika zažila během prezidentských voleb v roce 2023 mohutnou vlnu hackerských útoků typu DDoS (*Distributed Denial-of-Service*), jejichž cílem bylo zpomalit či úplně znefunkčnit webové stránky napadených organizací. Útočníci byli členy anonymní skupiny NoNamed057, kteří chtěli *"osvobodit"* Česko od lidí, kteří mají strach z Ruska a ruských lidí. Útoky se uskutečnily na weby prezidentských kandidátů, státních institucí, průmyslových podniků a nevládních organizací. Útočníci pokračovali v útocích i během prezidentských voleb a napadli i firmy podnikající ve zpracovatelském a hutním průmyslu.

Kyberútoky proti České republice

Po stopách neznámého útočníka

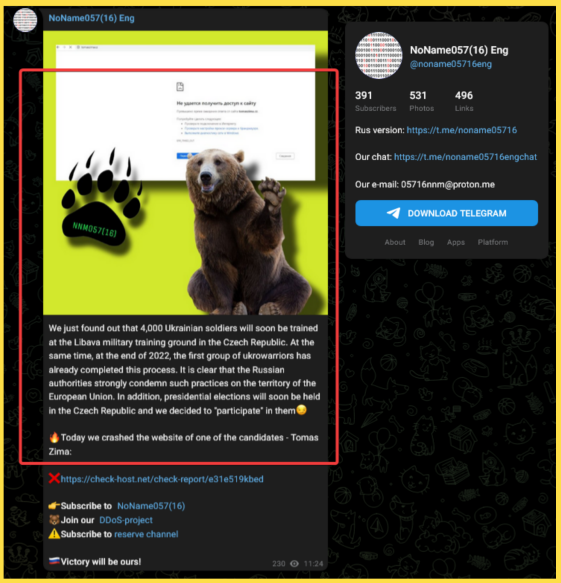


Česká republika zažila během nedávných prezidentských voleb mohutnou vlnu hackerských útoků typu DDoS (*Distributed Denial-of-Service*), jejichž cílem bylo zpomalit či úplně znefunkčnit webové stránky napadených organizací. Kromě internetových stránek některých prezidentských kandidátů byly cílem útoků rovněž weby několika klíčových státních institucí, včetně ministerstev. Napadené byly též weby významných průmyslových podniků a nevládních organizací. Weby byly po útocích buď zcela vyřazeny z provozu anebo útočníci způsobili jejich dočasné výpadky. Na fungování postižených organizací mají DDos útoky škodlivý vliv, neboť snižují jejich schopnost poskytovat návštěvníkům informace prostřednictvím internetu. Není jasné, kdo přesně za útoky stál, ale anonymní skupina NoNamed057, která se k útokům přihlásila uvedla, že jejich motivací bylo osvobodit Českou republiku od *"rusofobů"*, tj. od lidí, kteří cítí nenávist vůči Ruské federaci a ruským lidem a od lidí, kteří mají z Ruské federace a ruských lidí strach.

Analýza útoků a jejich příčin

Útočníci použili DDDoS útoky

Analýzou digitálních stop z veřejně dostupných zdrojů, tj. zejména veřejných skupin a kanálů na sociální síti Telegram jsme identifikovali, že DDoS útoky skupiny NoNamed057 proti cílům v České republice začaly s velkou mírou pravděpodobnosti v dopoledních hodinách ve středu dne 11. ledna 2023, kdy v důsledku DDoS útoku došlo k pádu webu jednoho z kandidátů v českých prezidentských volbách, Tomáše Zimy.



DDoS je zkratka z anglického Distributed Denial of Service, což česky znamená distribuované odepření služby. Při tomto typu kybernetického útoku je cílem útočníka znepřístupnit napadené webové stránky, a to tak, že je zahltí provozem. Na telegramovém kanálu na url adrese https://t.me/noname05716, který patří hacktivistické skupině NoNamed057 jsme ve středu dne 11. ledna 2023 v čase 11:24 identifikovali oznámení o tom, že se NoNamed057 právě dozvěděli, že na vojenském cvičišti Libavá v České republice bude brzy cvičit 4 000 ukrajinských vojáků.[1] Podobný výcvik

[1] *Zdroj: https://t.me/s/noname05716eng/369*

podle NoNamed057 prý v České republice absolvovala na konci roku 2022 již první skupina *“ukrowarriorů”* a je zřejmé, že úřady Ruské federace podobné praktiky na území Evropské unie důrazně odsuzují. V této souvislosti NoNamed057 na svém telegramovaném kanálu rovněž uvedli, že se v České republice prý brzy uskuteční prezidentské volby, a oni (NoNamed057) se jich rozhodli *"zúčastnit"* a právě dnes (pozn. ve středu dne 11. ledna 2023) *“nabourali webové stránky jednoho z kandidátů - Tomáše Zimy”*.

Datum a čas	Doména oběti	Url stopa útočníka
2023-01-11 11:24:00	tomaszima.cz	https://t.me/s/noname05716eng/369
		Zdroj: Telegram

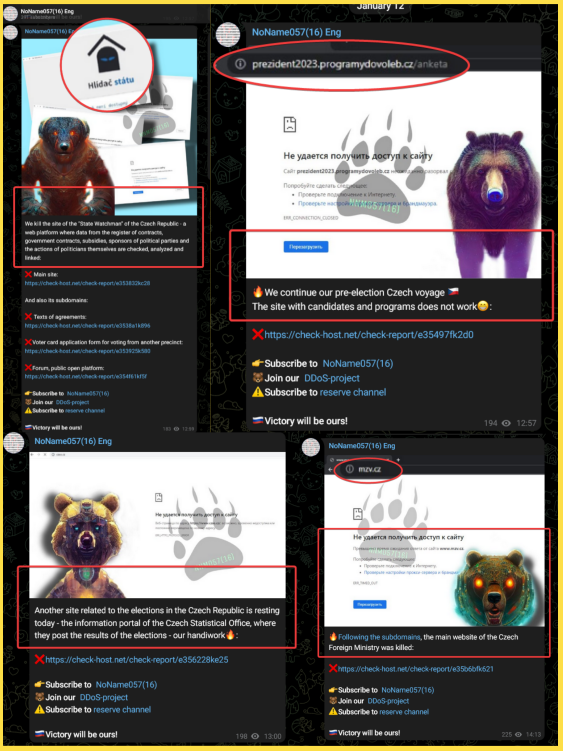
Anonymní skupina NoNamed057 praktikuje hacktivismus, což je používání či zneužívání počítačových technik jako je hacking, etický hacking, Google-hacking, Dorking, Doxing atd. coby forma občanské neposlušnosti k podpoře politického programu či společenské změny.[2]

První vlna útoků

čtvrtek 12. ledna 2013

Ve čtvrtek dne 12. ledna 2023 byly napadeny weby dvou českých nevládních organizací - Hlídač státu a Programy do voleb a dvě webové stránky klíčových státních institucí v Česku. Českého statistického úřadu, který hrál klíčovou roli při sčítání hlasů v prezidentských volbách web Ministerstva zahraničních věcí ČR. Hackerské útoky NoNamed057 neustaly ani přímo v průběhu prezidentských voleb v Česku ve dnech 13. a 14. ledna 2023.

Datum a čas	Doména oběti	Url stopa útočníka
2023-01-12 14:13:00	mzv.cz	https://t.me/s/noname05716eng/374
2023-01-12 13:02:00	mzv.cz	https://t.me/s/noname05716eng/373
2023-01-12 13:00:00	czso.cz	https://t.me/s/noname05716eng/372
2023-01-12 12:59:00	hlidacstatu.cz	https://t.me/s/noname05716eng/371
2023-01-12 12:57:00	programydovoleb.cz	https://t.me/s/noname05716eng/370
		Zdroj: Telegram



Útoky při prezidentských volbách I.

pátek 13. a sobota 14. ledna 2023

V pátek dne 13. ledna 2023 se skupina NoNamed057 na svém telegramovém kanálu pochlubila opětovným shozením internetových stránek jednoho z prezidentských kandidátů Tomáše Zimy a opakovala útoky na weby Ministerstva zahraničních věcí ČR a Hlídače státu.

Datum a čas	Doména oběti	Url stopa útočníka
2023-01-13 12:10:00	tomaszima.cz	https://t.me/s/noname05716eng/378
2023-01-13 10:18:00	hlidacstatu.cz	https://t.me/s/noname05716eng/376
2023-01-13 10:17:00	mzv.cz	https://t.me/s/noname05716eng/375
		Zdroj: Telegram

Útočníci napadli nevládní organizace Hlídač státu a Programy do voleb, které se v České republice obě zabývají veřejnou kontrolou státu a jeho institucí. Hlídač státu je veřejně prospěšný projekt, jehož cílem je kontrolovat státní a veřejné

[2] *Zdroj: https://en.wikipedia.org/wiki/Hacktivism*

instituce, a to pomocí aplikací Hlídač smluv, Registr smluv nebo Hlídač webů. Programy do voleb je pro změnu zájmový spolek, jehož cílem v inkriminované době bylo přinášet nestranný pohled na kandidáty v českých prezidentských volbách ve dnech 13. a 14. ledna 2023. Útočníci z NoNamed057 tuto veřejnou kontrolu narušili, čímž buď zcela zamezili nebo výrazně ztížili naplňovat hlavní poslání nevládních organizací v demokratických společnostech, tj. umožnit veřejnosti z řad tzv. občanské společnosti, aby se účastnila správy věcí veřejných. V sobotu dne 14. ledna 2023 byly opětovně napadeny webové stránky Hlídače státu a Českého statistického úřadu. Na ústředí sčítání volebních výsledků prvního kola prezidentských voleb v Česku zaútočili hackeři z NoNamed057 též v neděli dne 15. ledna 2023. V následujícím týdnu, tj. od 16. do 22. ledna 2023 pokračovali NoNamed057 v útocích na průmyslové podniky se sídlem v České republice.

Datum a čas	Doména oběti	Url stopa útočníka
2023-01-14 10:10:00	volby.cz	https://t.me/s/noname05716eng/379
2023-01-14 10:10:00	hlidacstatu.cz	https://t.me/s/noname05716eng/380
2023-01-15 13:36:00	volby.cz	https://t.me/s/noname05716eng/388
2023-01-15 13:36:00	volby.cz	https://t.me/s/noname05716eng/398
2023-01-15 10:36:00	czso.cz	https://t.me/s/noname05716eng/384
		Zdroj: Telegram

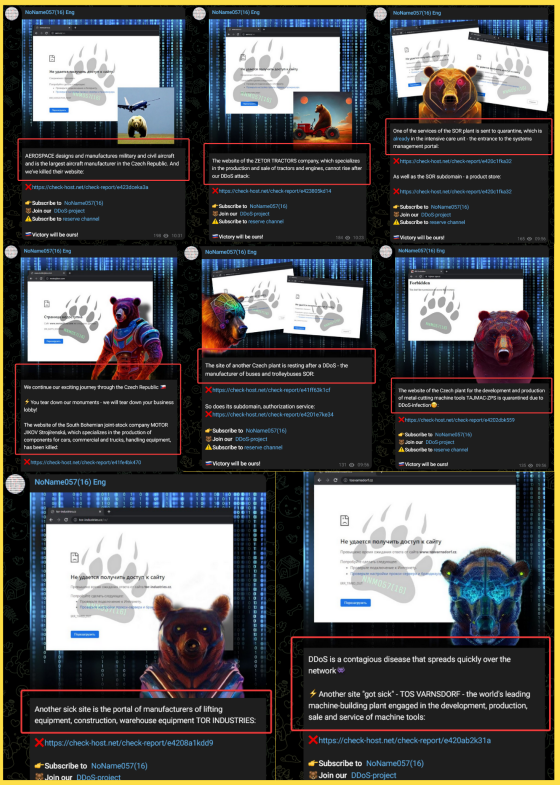
Útoky na český průmysl

pátek 16. až neděle 22. ledna 2023

V pondělí dne 16. ledna 2023 došlo k další sérii útoků, tentokrát na internetové domény vesměs soukromých obchodních společností a průmyslových podniků.

Datum a čas	Doména oběti	Url stopa útočníka
2023-01-16 10:31:00	aero.cz	https://t.me/s/noname05716eng/397
2023-01-16 10:23:00	zetor.cz	https://t.me/s/noname05716eng/396
2023-01-16 09:56:00	cals.cz	https://t.me/s/noname05716eng/395
2023-01-16 09:56:00	motorjikov.com	https://t.me/s/noname05716eng/390
2023-01-16 09:56:00	sor.cz	https://t.me/s/noname05716eng/391
2023-01-16 09:56:00	tajmac-zps.cz	https://t.me/s/noname05716eng/392
2023-01-16 09:56:00	tor-industries.cz	https://t.me/s/noname05716eng/393
2023-01-16 09:56:00	tosvarnsdorf.cz	https://t.me/s/noname05716eng/394
		Zdroj: Telegram

Terčem byly české průmyslové podniky AERO Vodochody AEROSPACE, ZETOR TRACTORS, CALS servis, MOTOR JIKOV Group, SOR Libchavy, TAJMAC - ZPS, TOR INDUSTRIES a TOS Varnsdorf.



Akciová společnost AERO Vodochody AEROSPACE je přední český výrobce vojenské a civilní letecké techniky s tradicí od roku 1919. Specializuje se na vývoj, montáž, výrobu a servis letadel. Akciová společnost ZETOR TRACTORS je přední český výrobce a dodavatel náhradních dílů a příslušenství pro traktory Zetor. Akciové společnosti MOTOR JIKOV Group, TAJMAC - ZPS, TOS Varnsdorf a společnost s ručením omezeným TOR INDUSTRIES podnikají ve strojírenství. Společnost s ručením omezeným CALS servis dodává počítačové technologie pro

zbrojní průmysl a společnost s ručením omezeným SOR Libchavy SOR Libchavy je významný český výrobce a prodejce autobusů pro městskou, meziměstskou a turistickou dopravu. Útoky pokračovaly celý týden a jejich cílem byly kromě obranného průmyslu a strojírenství též soukromé firmy podnikající ve zpracovatelském a hutním průmyslu.

Datum a čas	Doména oběti	Url stopa útočníka
2023-01-17 10:21:00	kovosvit.cz	https://t.me/s/noname05716eng/405
2023-01-17 10:02:00	retos.cz	https://t.me/s/noname05716eng/404
2023-01-17 09:44:00	fermatmachinery.com	https://t.me/s/noname05716eng/403
2023-01-17 09:43:00	emp-slavkov.cz	https://t.me/s/noname05716eng/402
2023-01-17 09:42:00	poldi-steel.com	https://t.me/s/noname05716eng/401
2023-01-17 09:40:00	pasovaocel.cz	https://t.me/s/noname05716eng/400
2023-01-17 09:39:00	pilous.cz	https://t.me/s/noname05716eng/399
		Zdroj: Telegram

V úterý dne 17. ledna 2023 se staly terčem hackerských útoku hacktivistické skupiny NoName057 webové stránky soukromých obchodních společností se sídlem v Česku PILOUS - pásové pily, Pásová ocel, Poldi Steel, EMP, FERMAT CZ, ReTOS Varnsdorf a KOVOSVIT MAS Machine Tools. Další vlna útoků zasáhla ve středu dne 18. ledna 2023 weby organizací Slovácké strojírny, strojírnu Šmeral Brno, Ministerstvo obrany ČR, a weby vládní agentury Czech Trade.

Datum a čas	Doména oběti	Url stopa útočníka
2023-01-18 14:31:00	czechtradeoffices.com	https://t.me/s/noname05716eng/416
2023-01-18 14:00:00	czechtrade.cz	https://t.me/s/noname05716eng/415
2023-01-18 13:30:00	czechtrade.cz	https://t.me/s/noname05716eng/414
2023-01-18 13:02:00	czechtrade.cz	https://t.me/s/noname05716eng/413
2023-01-18 12:30:00	czechtrade.cz	https://t.me/s/noname05716eng/412
2023-01-18 12:01:00	smeral.cz	https://t.me/s/noname05716eng/411
2023-01-18 11:03:00	army.cz	https://t.me/s/noname05716eng/409
2023-01-18 10:38:00	army.cz	https://t.me/s/noname05716eng/408
2023-01-18 10:25:00	army.cz	https://t.me/s/noname05716eng/407
2023-01-18 10:24:00	sub.cz	https://t.me/s/noname05716eng/406
		Zdroj: Telegram

Organizace CzechTrade spadá pod Ministerstvo průmyslu a obchodu České republiky a provozuje kanceláře českých obchodních zastoupení v zahraničí.

Datum a čas	Doména oběti	Url stopa útočníka
2023-01-19 11:50:00	mpo.cz	https://t.me/s/noname05716eng/422
2023-01-19 11:43:00	mdcr.cz	https://t.me/s/noname05716eng/421
2023-01-19 11:42:00	mdcr.cz	https://t.me/s/noname05716eng/420
2023-01-19 11:41:00	tajmac-zps.cz	https://t.me/s/noname05716eng/419
2023-01-19 11:40:00	jawa.eu	https://t.me/s/noname05716eng/418
2023-01-19 09:28:00	mfcr.cz	https://t.me/s/noname05716eng/417
		Zdroj: Telegram

Ve čtvrtek dne 19. ledna 2023 se NoNamed057 na svém telegramovém kanálu pochlubili opětovným útokem na strojírnu TAJMAC - ZPS. Napadli též web tradičního českého výrobce motocyklů JAWA Moto a pokračovali v útocích na ústřední orgány české státní správy. Zaměřili se na weby českého ministerstva financí, ministerstva dopravy a ministerstva průmyslu a obchodu. Útoky na ministerstvo průmyslu a obchodu pokračovaly i v pátek dne 20. ledna 2023.

Datum a čas	Doména oběti	Url stopa útočníka
2023-01-20 14:02:00	tosvarnsdorf.cz	https://t.me/s/noname05716eng/428
2023-01-20 13:14:00	ckd.cz	https://t.me/s/noname05716eng/427
2023-01-20 12:30:00	tstservis.cz	https://t.me/s/noname05716eng/426
2023-01-20 11:45:00	excaliburarmy.cz	https://t.me/s/noname05716eng/425
2023-01-20 11:09:00	mpo.cz	https://t.me/s/noname05716eng/424
2023-01-20 10:26:00	t-support.cz	https://t.me/s/noname05716eng/423
		Zdroj: Telegram

Pokračovaly též útoky na české průmyslové podniky. Kromě opětovného napadení strojírenské firmy TOS Varnsdorf se staly terčem útoků i další české strojírny jako ČKD GROUP a TST servis, dále technologická firma technology-support či další přední český výrobce zbraní a střeliva, zbrojařská firma EXCALIBUR ARMY.. O víkendu dne 21. a 22. ledna 2023 pokračovali hackeři z NoNamed057 v útocích na hutní závod

Poldi Steel, přední českou zbrojařskou firmu AERO Vodochody AEROSPACE a Ministerstvo obrany České republiky.

Datum a čas	Doména oběti	Url stopa útočníka
2023-01-21 16:47:00	poldi-steel.com	https://t.me/s/noname05716eng/438
2023-01-21 16:11:00	alfe.cz	https://t.me/s/noname05716eng/437
2023-01-21 15:10:00	weilercz.com	https://t.me/s/noname05716eng/436
2023-01-21 14:32:00	vanad.cz	https://t.me/s/noname05716eng/435
2023-01-21 13:21:00	kovopb.cz	https://t.me/s/noname05716eng/434
2023-01-21 12:07:00	aero.cz	https://t.me/s/noname05716eng/433
2023-01-21 09:13:00	tos.cz	https://t.me/s/noname05716eng/430
2023-01-21 08:35:00	toshulin.cz	https://t.me/s/noname05716eng/429
		Zdroj: Telegram

V sobotu dne 21. ledna 2023 oznámili na svém telegramovém kanálu, že shodili též weby sléváren ALFE BRNO, web Kovohutí Příbram nástupnické a českých strojírenských firem, WEILER Holoubkov, Vanad 2000, TOS Svitavy a TOSHULIN.

Datum a čas	Doména oběti	Url stopa útočníka
2023-01-22 15:50:00	army.cz	https://t.me/s/noname05716eng/447
2023-01-22 15:11:00	army.cz	https://t.me/s/noname05716eng/446
2023-01-22 14:36:00	army.cz	https://t.me/s/noname05716eng/444
2023-01-22 14:16:00	army.cz	https://t.me/s/noname05716eng/445
2023-01-22 12:25:00	army.cz	https://t.me/s/noname05716eng/443
2023-01-22 11:30:00	army.cz	https://t.me/s/noname05716eng/442
2023-01-22 10:45:00	army.cz	https://t.me/s/noname05716eng/441
2023-01-22 10:01:00	army.cz	https://t.me/s/noname05716eng/440
2023-01-22 09:26:00	army.cz	https://t.me/s/noname05716eng/439
		Zdroj: Telegram

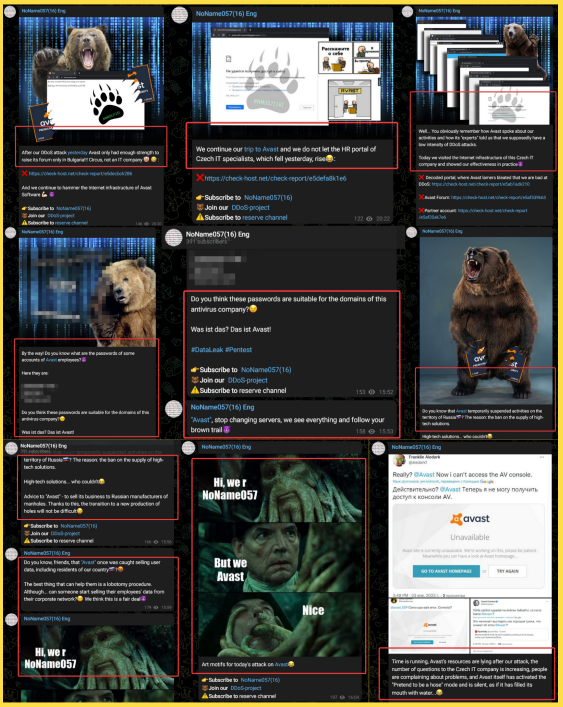
Útoky na Avast Software

pondělí 23. až úterý 24. ledna 2023

V pondělí dne 23. ledna 2023 napadli hackeři z NoNamed057 web české softwarové firmy Avast Software a odhalili hesla některých pracovníků. Útoky pokračovaly i v úterý dne 24. ledna 2023.

Datum a čas	Doména oběti	Url stopa útočníka
2023-01-23 16:34:00	avast.io	https://t.me/s/noname05716eng/459
2023-01-23 16:04:00	avast.io	https://t.me/s/noname05716eng/458
2023-01-23 15:59:00	avast.io	https://t.me/s/noname05716eng/457
2023-01-23 15:56:00	avast.io	https://t.me/s/noname05716eng/456
2023-01-23 15:53:00	avast.io	https://t.me/s/noname05716eng/455
2023-01-23 15:52:00	avast.io	https://t.me/s/noname05716eng/454
2023-01-23 15:03:00	avast.io	https://t.me/s/noname05716eng/453
2023-01-24 20:22:00	myworkdayjobs.com	https://t.me/s/noname05716eng/463
2023-01-24 20:20:00	avast.com	https://t.me/s/noname05716eng/462
		Zdroj: Telegram

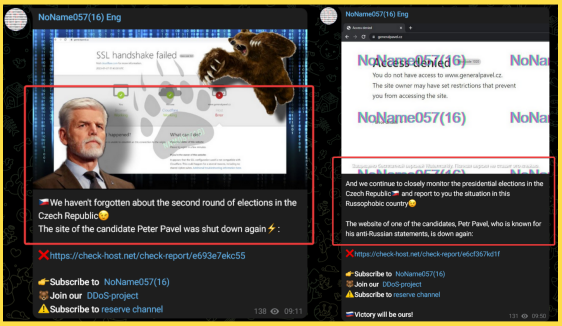
Společnost s ručením omezeným Avast Software je původem česká společnost zabývající se počítačovou a informační bezpečností. V oboru kyberbezpečnosti působí více než 25 let a je jednou z nejstarších firem v tomto odvětví. Má více než 1 700 zaměstnanců a podle objemu tržeb je druhou největší antivirovou firmou na světě. V září 2022 bylo oznámeno spojení českého Avastu s americkým technologickým gigantem Symantec Corporation (dříve Norton LifeLock).[3]



[3] *Zdroj: https://cs.wikipedia.org/wiki/Avast_Software*

Útoky při prezidentských volbách II.

pátek 27. a sobota 28. ledna 2023



Již v pátek dne 27. ledna 2023 v čase 9:11 uvedli hackeři z NoName057 na svém telegramovém účtu, že prý *"Nezapomněli na druhé kolo voleb (prezidentských) v České republice"* a při té příležitosti oznámili, že vyřadili z provozu web *generalpavel.cz* kandidáta a budoucího vítěze prezidentských voleb Petra Pavla.

Datum a čas	Doména oběti	Url stopa útočníka
2023-01-27 09:11:00	generalpavel.cz	https://t.me/s/noname05716eng/487
		Zdroj: Telegram

Petr Pavel je český politik a armádní generál ve výslužbě. Od ledna 2023 zvolený prezident České republiky. Úřadu se ujme složením slibu dne 9. března 2023 na společné schůzi obou komor Parlamentu. V letech 2012–2015 byl náčelníkem Generálního štábu Armády České republiky a mezi roky 2015 a 2018 působil ve funkci předsedy vojenského výboru NATO. Stal se tak prvním zástupcem zemí bývalé Varšavské smlouvy, který nastoupil do nejvyšší vojenské funkce Severoatlantické aliance. Se ziskem 35,40 % hlasů vyhrál první kolo přímé prezidentské volby v roce 2023. Ve druhém rozhodujícím kole zvítězil s 58,32 % hlasů nad Andrejem Babišem.

Datum a čas	Doména oběti	Url stopa útočníka
2023-01-27 09:11:00	generalpavel.cz	https://t.me/s/noname05716eng/487
2023-01-27 09:50:00	mzv.cz	https://t.me/s/noname05716eng/488
2023-01-27 10:26:00	hlidacstatu.cz	https://t.me/s/noname05716eng/489
2023-01-28 09:50:00	mzv.cz	https://t.me/s/noname05716eng/499
2023-01-28 09:50:00	volby.cz	https://t.me/s/noname05716eng/496
2023-01-28 10:20:00	generalpavel.cz	https://t.me/s/noname05716eng/495
2023-01-28 13:10:00	generalpavel.cz	https://t.me/s/noname05716eng/505
2023-01-29 13:30:00	czso.cz	https://t.me/s/noname05716eng/507
		Zdroj: Telegram

V průběhu druhého kola prezidentských voleb v České republice ve dnech 27. a 28. ledna 2023 omezili NoName057 kromě webu prezidentského kandidáty Petra Pavla opětovně i dostupnost webových stránek nevládní organizace Hlídač státu, a internetových stránek českého ministerstva zahraničních věcí a Českého statistického úřadu. Web s výsledky prezidentských voleb napadli opětovně i v neděli dne 29. ledna 2023.

Odveta za *"Mrtvého Rusa"*

čtvrtek 2. února 2023

Zatím poslední aktivitu NoName057 proti cílům v Česku jsme identifikovali ve čtvrtek dne 2. února 2023. V čase 13:15 zveřejnili NoName057 na svém teegramovém kanálu, že nabourali web

údajně *“rusofobního”* Havana Club Baru 23 v Praze. V tomto baru v centru české metropole, který podle internetových stránek patří firmě M E L M A R K s.r.o. se údajně rozhodli přejmenovat koktejl *"Bílý Rus"* na *"Mrtvý Rus" a* NoName057, to svými slovy *“zkrátka nemohli pominout”*.

Datum a čas	Doména oběti	Url stopa útočníka
2023-02-02 13:15:00	bar23.cz	https://t.me/s/noname05716eng/539

Zdroj: Telegram

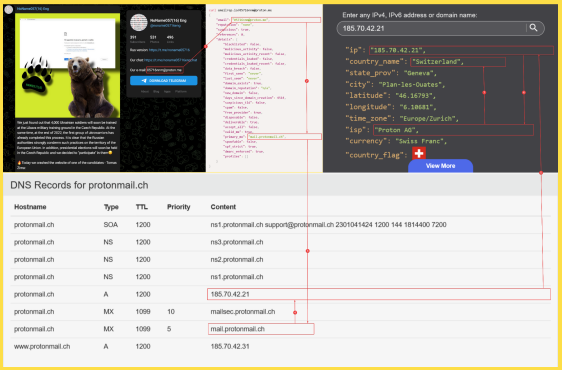
Aktivity NoNamed057 v oblasti kybernetické války proti *"rusofobním"* zemím jsou důvodem k obavám a mezinárodní společenství musí přijmout opatření proti této hrozbě, neboť státem podporovaný terorismus představuje vážnou hrozbu pro celý demokratický svět. Západní vlády a bezpečnostní organizace mají mnoho důvodů brát NoNamed057 skutečně vážně. V prosinci 2022 se NoNamed057 přihlásili k útokům na web Vlády Polské republiky. Jak poznamenala polská administrativa, incident byl reakcí na Sejm Polské republiky, který v polovině prosince 2022 oficiálně uznal Rusko jako státního sponzora terorismu. Ze stejných důvodů zaútočili NoNamed057 v polovině února na vládní weby Slovenska. Analýza telegramového kanálu skupiny NoName057 ukazuje, že tento útočník vyhledává uznání, čehož dosahuje tím, že na útoky odkazuje online, včetně článků na Wikipedii. Telegramový kanál NoName057 též zveřejňuje proruské memy, motivační příspěvky a pro kremelskou propagandu. Aktivity NoName057 se nejvíce podobají další prorusky orientované hacktivistické skupině Killnet. Ta nechvalně proslula DDoS útoky na vládní a soukromé instituce v několika prozápadních zemích během ruské invaze na Ukrajinu. Předpokládá se, že skupina Killnet vznikla někdy v březnu 2022. Jsou podezřelí, že se v roce 2022 pokusili zablokovat web hudební soutěže Eurovize (Eurovision Song Contest), a to během vystoupení soutěžících z Ukrajiny. V dubnu 2022 se Killnet přihlásil k útokům na weby v Česku, a to včetně veřejnoprávních médií (Česká Televize a Český rozhlas) a webu národního železničního dopravce (České Dráhy)[4],[5]. Z aktivit identifikovaných na Telegramu usuzujeme, že vedle veřejně známější skupiny Killnet, se za nejlepšího ruského aktéra hrozeb současnosti považují právě NoNamed057 a i když faktický dopad jejich DDoS útoků byl ve skutečnosti zatím krátkodobý nebo žádný nelze vyloučit, že po veřejné kritice budou jejich útoky nabývat na intenzitě i agresivitě, aby svou veřejně deklarovanou pozici NoNamed057 potvrdili též v praxi.

Pokusy o odhalení

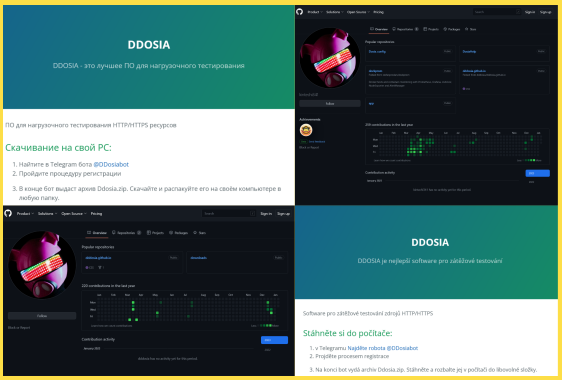
Zatím neúspěšné

Skupina NoNamed057 je známá schopností skrývat skutečnou identitu svých hlavních představitelů a spolupracovníků. K tomu paradoxně zneužívá internetových nástrojů a služeb, které vyvinuli lidé v prozápadně orientovaných zemích proti kterým útočí. Pokusy o vystopování, odhalení a neutralizaci NoNamed057 zatím nebyly úspěšné. Na základě analýzy dostupných informací jsme identifikovali, že telegramový kanál skupiny NoName057 je úzce propojený s e-mailovým účtem, jehož adresa je 05716nnm@proton.me.

[4] *Zdroj: https://en.wikipedia.org/wiki/Killnet*
[5] *Zdroj: https://www.expats.cz/czech-news/article/czech-television-hit-in-another-wave-of-cyber-attacks*



Identifikovali jsme, že e-mailový účet 05716nnm@proton.me byl s velkou mírou pravděpodobnosti aktivován v sobotu dne 27. srpna 2022. Prostor pro hostování mu poskytl poštovní server mail.protonmail.ch, který provozuje firma Proton AG se sídlem ve Švýcarsku. Proton AG je technologická společnost nabízející online služby zaměřené na ochranu soukromí. Firma Proton AG byla založena v roce 2014 skupinou vědců, kteří se setkali v CERNu, což je největší laboratoř částicové fyziky na světě.[6],[7] Služby poskytovatele Proton AG včetně elektronické pošty Proton Mail jsou mezi uživateli internetu vyhledávány a vysoce ceněny zejména pro svou schopnost ochránit/skrýt skutečnou identitu uživatelů.



Pro vývoj a šíření svých produktů používali NoName057 komunitní platformu GitHub od stejnojmenné počítačové firmy se sídlem v Kalifornii v USA, která je od roku 2018 součástí nadnárodního technologického gigantu Microsoft.

[6] *Zdroj: https://en.wikipedia.org/wiki/CERN*
[7] *Zdroj: https://en.wikipedia.org/wiki/Proton_AG*

GitHub se používá k hostování projektů a vývoji softwaru s tzv. otevřeným zdrojovým kódem.[8] K lednu 2023 měl GitHub více než 100 milionů vývojářů 372 milionů repozitářů a nejméně 28 milionů veřejných úložišť, což z něj dělá největšího hostitele zdrojového kódu na světě vůbec NoName057 používali GitHub k vývoji a šíření bezplatných DDoS nástrojů které hostovali na adrese https//dddosia.github.io pod uživatelskými jmény dddosia a kintechi341.[9],[10] Po upozornění výzkumníků a bezpečnostních expertů, že na GitHubu provozují nezákonné aktivity jim GitHub účty zrušil.

Роман Омельченко

„Пластун“

Někteří internetoví výzkumníci a bezpečnostní experti uvádějí, že spolutvůrcem škodlivého DDDos programu byl uživatel GitHubu *„Роман Омельченко“*. Původní předpoklad, že by se mohlo jednat o reálného uživatele se ovšem nepotvrdil.

P.č.	Služba	Url Profil	Mobil
1.	Facebook	https://www.facebook.com/profile.php?id=10******** 87461	79******96888
2.	Facebook	https://www.facebook.com/profile.php?id=10******** 72757	79******37585
3.	Facebook	https://www.facebook.com/profile.php?id=10******** 43146	18******90390
4.	Facebook	https://www.facebook.com/profile.php?id=10******** 82981	79******21000
5.	Facebook	https://www.facebook.com/profile.php?id=10******** 64512	79******71044
6.	Facebook	https://www.facebook.com/profile.php?id=10******** 92176	79******46111
7.	Facebook	https://www.facebook.com/profile.php?id=10******** 45263	79******77700
8.	Facebook	https://www.facebook.com/profile.php?id=10******** 32575	79******02439
9.	Facebook	https://www.facebook.com/profile.php?id=10******** 14171	97******230204
10.	Facebook	https://www.facebook.com/profile.php?id=10******** 95662	79******85785
11.	Facebook	https://www.facebook.com/profile.php?id=10******** 90379	79******73470
12.	Facebook	https://www.facebook.com/profile.php?id=15********	16******79206
13.	Facebook	https://www.facebook.com/profile.php?id=15********	79******92323
14.	Facebook	https://www.facebook.com/profile.php?id=15********	79******79092
15.	Linkedin	https://linkedin.com/in/roman-omelchenko-87********	Unknown

[8] *Zdroj: https://en.wikipedia.org/wiki/GitHub*
[9] *Zdroj: https//github.com/dddosia*
[10] *Zdroj: https//github.com/kintechi341*

P.č.	Služba	Url Profil	Mobil
16.	Linkedin	https://linkedin.com/in/roman-omelchenko-1b*******	Unknown
17.	Linkedin	https://linkedin.com/in/roman-omelchenko-9b*******	Unknown
18.	Linkedin	https://linkedin.com/in/roman-omelchenko-0a*******	Unknown
19.	Linkedin	https://linkedin.com/in/roman-omelchenko-3b*******	Unknown
20.	Linkedin	https://linkedin.com/in/roman-omelchenko-20*******	Unknown
21.	Linkedin	https://linkedin.com/in/roman-omelchenko********	Unknown
22.	Linkedin	https://linkedin.com/in/roman-omelchenko-b0*******	Unknown
23.	Linkedin	https://linkedin.com/in/roman-omelchenko-0b*******	Unknown
24.	Linkedin	https://linkedin.com/in/roman-omelchenko-92*******	Unknown
25.	Linkedin	https://linkedin.com/in/roman-omelchenko-b5*******	Unknown
26.	Linkedin	https://linkedin.com/in/roman-omelchenko-a9*******	Unknown

Zdroj: Facebook, LinkedIn

Na internetu jsme identifikovali více osob stejného jména, ale nikoho s prokazatelnými vazbami na NoName057.

Na základě průzkumu ruskojazyčných a ukrajinských zdrojů jsme dospěli k závěru, že *“Роман Омельченко”* je s velkou mírou pravděpodobnosti přezdívka inspirovaná skutečnou osobou. Jméno *„Роман Омельченко“* se podařilo spojit se skutečnou identitou proruského separatistického bojovníka, který byl aktivní v operacích v doněcké a luhanské oblasti již od roku 2014. Přesto, že byl několikrát prohlášen za padlého, poslední ověřená informace k jeho osobě se objevila v létě 2021. Pro proruský web *„Argumenty“* komentoval *„blížící se útok ukrajinské armády“* proti Donbasu.[11] Dotyčný povstalec *„Роман Омельченко“* je v řadách proruských sil a jejich sympatizantů znám jako respektovaný válečník s přezdívkou *„Пластун“* (*„Plastun“*).[12] Mediálně je prezentovný jako *„разведчик“*, v českém překladu průzkumník tedy příslušník pozemního vojska nebo zpravodajského oddělení se specializací zvěd nebo osoba provádějící vojenský průzkum. Neexistují zprávy ani indicie o jeho zapojení do kybernetických operací. S ohledem na zjištěné se domníváme, že uživatelský profil *„Роман Омельченко“* spojený s aktivitami skupiny NoName057 na GitHubu je fiktivní a s velkou mírou pravděpodobnosti využívaný anonymním hackerským aktivistou, který může být inspirován pověstí a kreditem proruského bojovníka jménem *„Роман Омельченко“* přezdívaného *„Пластун“*.

[11] *Zdroj: https://argumenti.ru/world/2021/04/716587*
[12] *Zdroj:https://politcentr.ru/16647-razvedchik-armii-dnr-roman-plastun-ob-ukrainskih-naemnikah-mezhdu-berdyanskom-i-mariupolem-est-dazhe-igilovcy.html*

Závěr a doporučení

Zůstat ve střehu

Předpokládá se, že NoName057 mají vazby na ruskou vládu a operují se státní podporou. V České republice zaútočili poté, kdy Ruská federace odsoudila výcvik ukrajinských vojáků v Česku. Problematika státem podporovaných hackerských skupin vyžaduje koordinované úsilí mezinárodního společenství. Demokratické vlády a organizace musí spolupracovat, aby zlepšily svou kybernetickou obranu a uměly čelit hrozbám, které představují skupiny jako NoNamed057. Považujeme za důležité zdůraznit, že mezi zasaženými doménami se nachází i domény orgánů české státní správy, které výrazně zasahují anebo koordinují zahraniční obranně-průmyslovou pomoc Ruskem napadené Ukrajině. Jde o česká ministerstva zahraničních věcí, ministerstvo obrany, ministerstvo průmyslu a obchodu, ministerstvo financí či ministerstvo dopravy. Současně byly zasažené i domény, které zahrnují servery českých průmyslových podniků, které se na výrobě vojenského materiálu podílejí buď přímo nebo prostřednictvím dodavatelského řetězce. Nelze tedy

vyloučit, že v souvislosti s DDOS útoky proti cílům v Česku mohlo jít o mapování prostředí pro budoucí útoky nebo dokonce o zastírací manévr. Důrazně doporučujeme zůstat ostražitý a být si vědom metod, které skupiny jako NoNamed057 používají k infiltraci systémů a následným krádežím citlivých informací. Útoky způsobily postiženým organizacím problémy, ale z našich aktuálních poznatků nevyplývá, že by útoky typu DDOS způsobené útočníkem NoName057 způsobily úniky citlivých dat nebo informací.

O nás

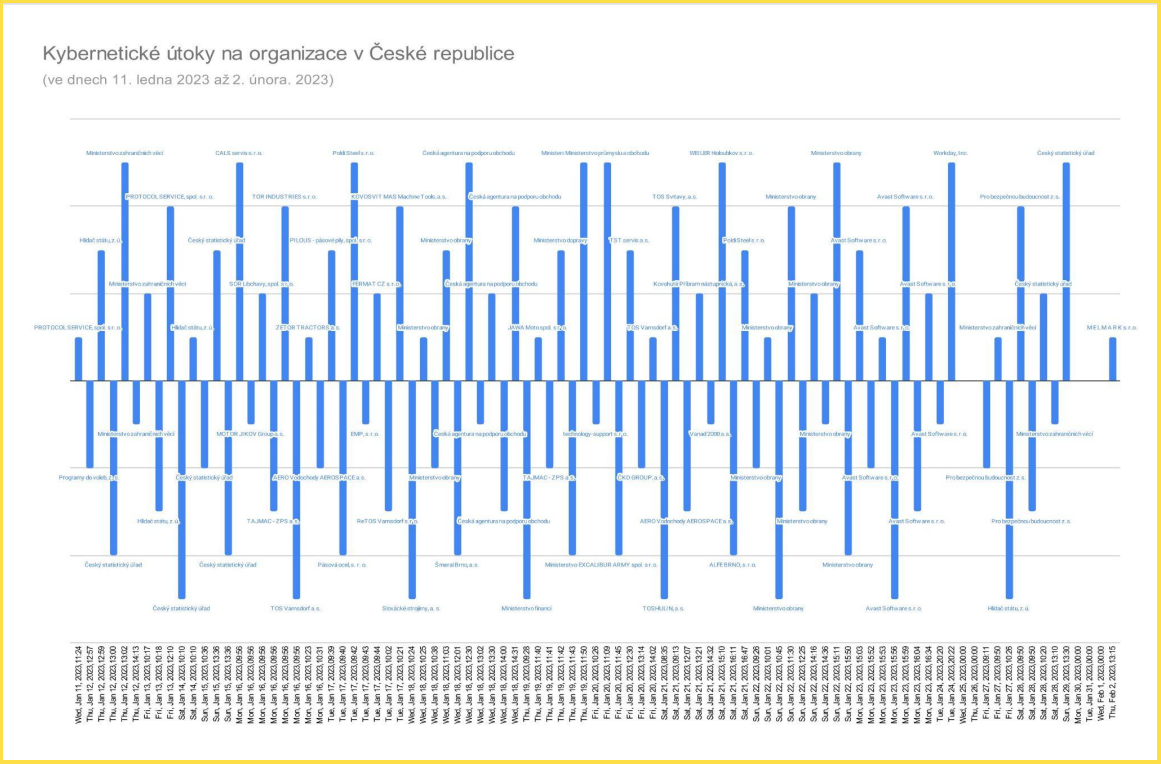
CZECHMATE CZ, s.r.o. je tým zkušených digitálních detektivů, kteří monitorují úniky citlivých informací jednotlivců a organizací na internet Specializují se na sběr a analýzu digitálních stop. Vyhodnocují hrozby, které mohou subjektu způsobit internetoví zločinci či konkurence a tim pomáhají předcházet a minimalizovat škody (dále jen *„CZECHMATE CZ“*). Na základě Smlouvy o partnerství s obchodní firmou NSHC PTE. LTD. (Singapore) má výhradní licenci pro užívání nástroje umělé inteligence DarkTracer pro sledování kriminálních aktivit na internetu s právem poskytovat sublicence dalším subjektům.[13] Všechna zjištění v tomto materiálu pocházejí z dat získaných nástrojem DarkTracer a analytickou činností CZECHMATE CZ .[14,15]

Upozornění

Upozorňujeme, že tento dokument obsahuje důvěrné informace a je určen výhradně pověřeným pracovníkům Klienta. Nesmí být bez předchozího souhlasu CZECHMATE CZ zpřístupněn třetí osobě, ani použít pro jiné účely. Všechny známky a názvy produktů v tomto materiálu jsou či mohou být registrované obchodní značky či obchodní a ochranné známky vlastníků.

[13] *Zdroj: https://darktracer.com/*
[14] *Zdroj: https://www.czechmatecz.com*
[15] *Zdroj: https://en.nshc.net/*

Přílohy:



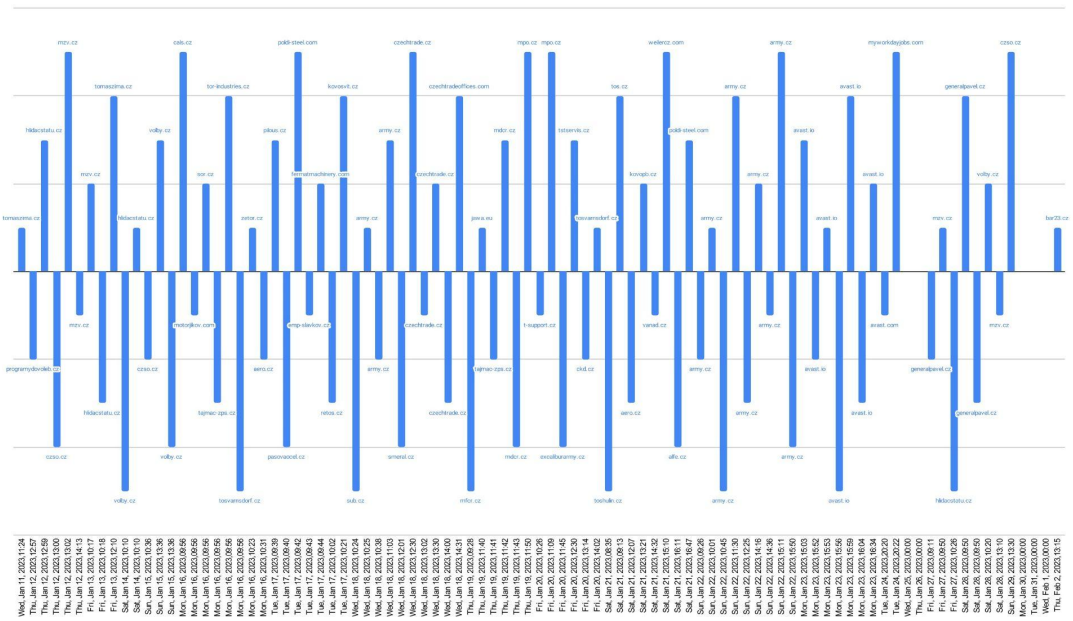
P. č.	Den	Datum a čas	Doména oběti	Napadená organizace	IČ	Url stopa útočníka
1.	středa	2023-01-11 11:24:00	tomaszima.cz	PROTOCOL SERVICE, spol. s r. o.	25722361	https://t.me/s/noname05716eng/369
2.	čtvrtek	2023-01-12 12:57:00	programydovoleb.cz	Programy do voleb, z. s.	10906380	https://t.me/s/noname05716eng/370
3.	čtvrtek	2023-01-12 12:59:00	hlidacstatu.cz	Hlídač státu, z.ú.	05965527	https://t.me/s/noname05716eng/371
4.	čtvrtek	2023-01-12 13:00:00	czso.cz	Český statistický úřad	00025593	https://t.me/s/noname05716eng/372
5.	čtvrtek	2023-01-12 13:02:00	mzv.cz	Ministerstvo zahraničních věcí	45769851	https://t.me/s/noname05716eng/373
6.	čtvrtek	2023-01-12 14:13:00	mzv.cz	Ministerstvo zahraničních věcí	45769851	https://t.me/s/noname05716eng/374
7.	pátek	2023-01-13 10:17:00	mzv.cz	Ministerstvo zahraničních věcí	45769851	https://t.me/s/noname05716eng/375
8.	pátek	2023-01-13 10:18:00	hlidacstatu.cz	Hlídač státu, z.ú.	05965527	https://t.me/s/noname05716eng/376
9.	pátek	2023-01-13 12:10:00	tomaszima.cz	PROTOCOL SERVICE, spol. s r. o.	25722361	https://t.me/s/noname05716eng/378
10.	sobota	2023-01-14 10:10:00	volby.cz	Český statistický úřad	00025593	https://t.me/s/noname05716eng/379
11.	sobota	2023-01-14 10:10:00	hlidacstatu.cz	Hlídač státu, z.ú.	05965527	https://t.me/s/noname05716eng/380
12.	neděle	2023-01-15 10:36:00	czso.cz	Český statistický úřad	00025593	https://t.me/s/noname05716eng/384
13.	neděle	2023-01-15 13:36:00	volby.cz	Český statistický úřad	00025593	https://t.me/s/noname05716eng/388
14.	neděle	2023-01-15 13:36:00	volby.cz	Český statistický úřad	00025593	https://t.me/s/noname05716eng/398
15.	pondělí	2023-01-16 09:56:00	cals.cz	CALS servis s.r.o.	26285002	https://t.me/s/noname05716eng/395
16.	pondělí	2023-01-16 09:56:00	motorjikov.com	MOTOR JIKOV Group a.s.	62525182	https://t.me/s/noname05716eng/390
17.	pondělí	2023-01-16 09:56:00	sor.cz	SOR Libchavy, spol. s r.o.	15030865	https://t.me/s/noname05716eng/391
18.	pondělí	2023-01-16 09:56:00	tajmac-zps.cz	TAJMAC - ZPS a.s.	26215578	https://t.me/s/noname05716eng/392
19.	pondělí	2023-01-16 09:56:00	tor-industries.cz	TOR INDUSTRIES s.r.o.	07323336	https://t.me/s/noname05716eng/393
20.	pondělí	2023-01-16 09:56:00	tosvarnsdorf.cz	TOS Varnsdorf a.s.	27327850	https://t.me/s/noname05716eng/394
21.	pondělí	2023-01-16 10:23:00	zetor.cz	ZETOR TRACTORS a.s.	26921782	https://t.me/s/noname05716eng/396
22.	pondělí	2023-01-16 10:31:00	aero.cz	AERO Vodochody AEROSPACE a.s.	24194204	https://t.me/s/noname05716eng/397
23.	úterý	2023-01-17 09:39:00	pilous.cz	PILOUS - pásové pily, spol. s r.o.	60727551	https://t.me/s/noname05716eng/399
24.	úterý	2023-01-17 09:40:00	pasovaocel.cz	Pásová ocel, s. r. o.	25614053	https://t.me/s/noname05716eng/400
25.	úterý	2023-01-17 09:42:00	poldi-steel.com	Poldi Steel s.r.o.	10969608	https://t.me/s/noname05716eng/401
26.	úterý	2023-01-17 09:43:00	emp-slavkov.cz	EMP, s.r.o.	44963912	https://t.me/s/noname05716eng/402
27.	úterý	2023-01-17 09:44:00	fermatmachinery.com	FERMAT CZ s.r.o.	26180367	https://t.me/s/noname05716eng/403
28.	úterý	2023-01-17 10:02:00	retos.cz	ReTOS Varnsdorf s.r.o.	62739204	https://t.me/s/noname05716eng/404
29.	úterý	2023-01-17 10:21:00	kovosvit.cz	KOVOSVIT MAS Machine Tools, a.s.	07333536	https://t.me/s/noname05716eng/405
30.	středa	2023-01-18 10:24:00	sub.cz	Slovácké strojírny, a. s.	00008702	https://t.me/s/noname05716eng/406

P. č.	Den	Datum a čas	Doména oběti	Napadená organizace	IČ	Url stopa útočníka
31.	středa	2023-01-18 10:25:00	army.cz	Ministerstvo obrany	60162694	https://t.me/s/noname05716eng/407
32.	středa	2023-01-18 10:38:00	army.cz	Ministerstvo obrany	60162694	https://t.me/s/noname05716eng/408
33.	středa	2023-01-18 11:03:00	army.cz	Ministerstvo obrany	60162694	https://t.me/s/noname05716eng/409
34.	středa	2023-01-18 12:01:00	smeral.cz	Šmeral Brno, a.s.	46346139	https://t.me/s/noname05716eng/411
35.	středa	2023-01-18 12:30:00	czechtrade.cz	Česká agentura na podporu obchodu	00001171	https://t.me/s/noname05716eng/412
36.	středa	2023-01-18 13:02:00	czechtrade.cz	Česká agentura na podporu obchodu	00001171	https://t.me/s/noname05716eng/413
37.	středa	2023-01-18 13:30:00	czechtrade.cz	Česká agentura na podporu obchodu	00001171	https://t.me/s/noname05716eng/414
38.	středa	2023-01-18 14:00:00	czechtrade.cz	Česká agentura na podporu obchodu	00001171	https://t.me/s/noname05716eng/415
39.	středa	2023-01-18 14:31:00	czechtradeoffices.com	Česká agentura na podporu obchodu	00001171	https://t.me/s/noname05716eng/416
40.	čtvrtek	2023-01-19 09:28:00	mfcr.cz	Ministerstvo financí	00006947	https://t.me/s/noname05716eng/417
41.	čtvrtek	2023-01-19 11:40:00	jawa.eu	JAWA Moto spol. s r. o.	25108743	https://t.me/s/noname05716eng/418
42.	čtvrtek	2023-01-19 11:41:00	tajmac-zps.cz	TAJMAC - ZPS a.s.	26215578	https://t.me/s/noname05716eng/419
43.	čtvrtek	2023-01-19 11:42:00	mdcr.cz	Ministerstvo dopravy	66003008	https://t.me/s/noname05716eng/420
44.	čtvrtek	2023-01-19 11:43:00	mdcr.cz	Ministerstvo dopravy	66003008	https://t.me/s/noname05716eng/421
45.	čtvrtek	2023-01-19 11:50:00	mpo.cz	Ministerstvo průmyslu a obchodu	47609109	https://t.me/s/noname05716eng/422
46.	pátek	2023-01-20 10:26:00	t-support.cz	technology-support s.r.o.	27106471	https://t.me/s/noname05716eng/423
47.	pátek	2023-01-20 11:09:00	mpo.cz	Ministerstvo průmyslu a obchodu	47609109	https://t.me/s/noname05716eng/424
48.	pátek	2023-01-20 11:45:00	excaliburarmy.cz	EXCALIBUR ARMY spol. s r.o.	64573877	https://t.me/s/noname05716eng/425
49.	pátek	2023-01-20 12:30:00	tstservis.cz	TST servis a.s.	00548880	https://t.me/s/noname05716eng/426
50.	pátek	2023-01-20 13:14:00	ckd.cz	ČKD GROUP, a.s.	27129357	https://t.me/s/noname05716eng/427
51.	pátek	2023-01-20 14:02:00	tosvarnsdorf.cz	TOS Varnsdorf a.s.	27327850	https://t.me/s/noname05716eng/428
52.	sobota	2023-01-21 08:35:00	toshulin.cz	TOSHULIN, a.s.	25510851	https://t.me/s/noname05716eng/429
53.	sobota	2023-01-21 09:13:00	tos.cz	TOS Svitavy, a.s.	15034020	https://t.me/s/noname05716eng/430
54.	sobota	2023-01-21 12:07:00	aero.cz	AERO Vodochody AEROSPACE a.s.	24194204	https://t.me/s/noname05716eng/433
55.	sobota	2023-01-21 13:21:00	kovopb.cz	Kovohutě Příbram nástupnická, a.s.	27118100	https://t.me/s/noname05716eng/434
56.	sobota	2023-01-21 14:32:00	vanad.cz	Vanad 2000 a.s.	25947575	https://t.me/s/noname05716eng/435
57.	sobota	2023-01-21 15:10:00	weilercz.com	WEILER Holoubkov s.r.o.	26315785	https://t.me/s/noname05716eng/436
58.	sobota	2023-01-21 16:11:00	alfe.cz	ALFE BRNO, s.r.o.	45475164	https://t.me/s/noname05716eng/437
59.	sobota	2023-01-21 16:47:00	poldi-steel.com	Poldi Steel s.r.o.	10969608	https://t.me/s/noname05716eng/438
60.	neděle	2023-01-22 09:26:00	army.cz	Ministerstvo obrany	60162694	https://t.me/s/noname05716eng/439
61.	neděle	2023-01-22 10:01:00	army.cz	Ministerstvo obrany	60162694	https://t.me/s/noname05716eng/440
62.	neděle	2023-01-22 10:45:00	army.cz	Ministerstvo obrany	60162694	https://t.me/s/noname05716eng/441
63.	neděle	2023-01-22 11:30:00	army.cz	Ministerstvo obrany	60162694	https://t.me/s/noname05716eng/442
64.	neděle	2023-01-22 12:25:00	army.cz	Ministerstvo obrany	60162694	https://t.me/s/noname05716eng/443
65.	neděle	2023-01-22 14:16:00	army.cz	Ministerstvo obrany	60162694	https://t.me/s/noname05716eng/445
66.	neděle	2023-01-22 14:36:00	army.cz	Ministerstvo obrany	60162694	https://t.me/s/noname05716eng/444
67.	neděle	2023-01-22 15:11:00	army.cz	Ministerstvo obrany	60162694	https://t.me/s/noname05716eng/446
68.	neděle	2023-01-22 15:50:00	army.cz	Ministerstvo obrany	60162694	https://t.me/s/noname05716eng/447
69.	pondělí	2023-01-23 15:03:00	avast.io	Avast Software s.r.o.	02176475	https://t.me/s/noname05716eng/453
70.	pondělí	2023-01-23 15:52:00	avast.io	Avast Software s.r.o.	02176475	https://t.me/s/noname05716eng/454
71.	pondělí	2023-01-23 15:53:00	avast.io	Avast Software s.r.o.	02176475	https://t.me/s/noname05716eng/455
72.	pondělí	2023-01-23 15:56:00	avast.io	Avast Software s.r.o.	02176475	https://t.me/s/noname05716eng/456
73.	pondělí	2023-01-23 15:59:00	avast.io	Avast Software s.r.o.	02176475	https://t.me/s/noname05716eng/457
74.	pondělí	2023-01-23 16:04:00	avast.io	Avast Software s.r.o.	02176475	https://t.me/s/noname05716eng/458
75.	pondělí	2023-01-23 16:34:00	avast.io	Avast Software s.r.o.	02176475	https://t.me/s/noname05716eng/459
76.	úterý	2023-01-24 20:20:00	avast.com	Avast Software s.r.o.	02176475	https://t.me/s/noname05716eng/462
77.	úterý	2023-01-24 20:22:00	myworkdayjobs.com	Workday, Inc.		https://t.me/s/noname05716eng/463
78.	pátek	2023-01-27 09:11:00	generalpavel.cz	Pro bezpečnou budoucnost z.s.	08749981	https://t.me/s/noname05716eng/487
79.	pátek	2023-01-27 09:50:00	mzv.cz	Ministerstvo zahraničních věcí	45769851	https://t.me/s/noname05716eng/488
80.	pátek	2023-01-27 10:26:00	hlidacstatu.cz	Hlídač státu, z.ú.	05965527	https://t.me/s/noname05716eng/489
81.	sobota	2023-01-28 09:50:00	generalpavel.cz	Pro bezpečnou budoucnost z.s.	08749981	https://t.me/s/noname05716eng/495
82.	sobota	2023-01-28 09:50:00	generalpavel.cz	Pro bezpečnou budoucnost z.s.	08749981	https://t.me/s/noname05716eng/505
83.	sobota	2023-01-28 10:20:00	volby.cz	Český statistický úřad	00025593	https://t.me/s/noname05716eng/496
84.	sobota	2023-01-28 13:10:00	mzv.cz	Ministerstvo zahraničních věcí	45769851	https://t.me/s/noname05716eng/499
85.	neděle	2023-01-29 13:30:00	czso.cz	Český statistický úřad	00025593	https://t.me/s/noname05716eng/507
86.	čtvrtek	2023-02-02 13:15:00	bar23.cz	M E L M A R K s.r.o.	49704877	https://t.me/s/noname05716eng/539

Zdroj: Telegram, CZECHMATE CZ s.r.o

Kybernetické útoky na weby v České republice

(ve dnech 11. ledna 2023 až 2. února. 2023)



P. č.	Den	Datum a čas	Napadená organizace	Vzkaz útočníka oběti
1.	středa	2023-01-11 11:24:00	PROTOCOL SERVICE, spol. s r. o.	We just found out that 4,000 Ukrainian soldiers will soon be trained at the Libava military training ground in the Czech Republic. At the same time, at the end of 2022, the first group of ukrowarriors has already completed this process. It is clear that the Russian authorities strongly condemn such practices on the territory of the European Union. In addition, presidential elections will soon be held in the Czech Republic and we decided to "participate" in them😏🔥Today we crashed the website of one of the candidates - Tomas Zima
2.	čtvrtek	2023-01-12 12:57:00	Programy do voleb, z. s.	We continue our pre-election Czech voyage 🇨🇿 The site with candidates and programs does not work😬
3.	čtvrtek	2023-01-12 12:59:00	Hlídač státu, z.ú.	We kill the site of the "State Watchman" of the Czech Republic - a web platform where data from the register of contracts, government contracts, subsidies, sponsors of political parties and the actions of politicians themselves are checked, analyzed and linked
4.	čtvrtek	2023-01-12 13:00:00	Český statistický úřad	Another site related to the elections in the Czech Republic is resting today - the information portal of the Czech Statistical Office, where they post the results of the elections - our handiwork🔥
5.	čtvrtek	2023-01-12 13:02:00	Ministerstvo zahraničních věcí	After our attacks, two subdomains of the Czech Foreign Ministry have been exhausted today
6.	čtvrtek	2023-01-12 14:13:00	Ministerstvo zahraničních věcí	Following the subdomains, the main website of the Czech Foreign Ministry was killed
7.	pátek	2023-01-13 10:17:00	Ministerstvo zahraničních věcí	We continue the Czech voyage 🇨🇿 - again we flood the Ministry of Foreign Affairs website with DDoS missiles🔥
8.	pátek	2023-01-13 10:18:00	Hlídač státu, z.ú.	We are wondering what the Czech portal "State Watchman" guards? Well, definitely not the site and subdomains from DDoS😉
9.	pátek	2023-01-13 12:10:00	PROTOCOL SERVICE, spol. s r. o.	Elections are in full swing in the Czech Republic, and websites are chasing our DDoS attack😉 Website of candidate Tomáš Zima
10.	sobota	2023-01-14 10:10:00	Český statistický úřad	Voting days continue 🇨🇿We vote for the Czech Republic free from Russophobes! Therefore, today we've sent ddos-grad to the sites: ❌Statistical information portal of the Czech Statistical Office with election results:
11.	sobota	2023-01-14 10:10:00	Hlídač státu, z.ú.	We still didn't understand what the State Watchman portal is for, so we've ddosed one more of its subdomains - an open platform for cooperation between the state, the public and companies
12.	neděle	2023-01-15 10:36:00	Český statistický úřad	Again, we send DDoS-missiles to the Czech statistical portal CZSO with the election results
13.	neděle	2023-01-15 13:36:00	Český statistický úřad	Another Czech portal with reports and voting results went to rest🔥
14.	neděle	2023-01-15 13:36:00	Český statistický úřad	Another Czech portal with reports and voting results went to rest🔥
15.	pondělí	2023-01-16 09:56:00	CALS servis s.r.o.	One of the services of the SOR plant is sent to quarantine, which is already in the intensive care unit - the entrance to the systems management portal:
16.	pondělí	2023-01-16 09:56:00	MOTOR JIKOV Group a.s.	We continue our exciting journey through the Czech Republic 🇨🇿 ⚡You tear down our monuments - we will tear down your business lobby! The website of the South Bohemian joint-stock company MOTOR JIKOV Strojírenská, which specializes in the production of components for cars, commercial and trucks, handling equipment, has been killed:
17.	pondělí	2023-01-16 09:56:00	SOR Libchavy, spol. s r.o.	The site of another Czech plant is resting after a DDoS - the manufacturer of buses and trolleybuses SOR
18.	pondělí	2023-01-16 09:56:00	TAJMAC - ZPS a.s.	The website of the Czech plant for the development and production of metal-cutting machine tools TAJMAC-ZPS is quarantined due to DDoS-infection😉
19.	pondělí	2023-01-16 09:56:00	TOR INDUSTRIES s.r.o.	Another sick site is the portal of manufacturers of lifting equipment, construction, warehouse equipment TOR INDUSTRIES
20.	pondělí	2023-01-16 09:56:00	TOS Varnsdorf a.s.	DDoS is a contagious disease that spreads quickly over the network👾 ⚡Another site "got sick" - TOS

P. č.	Den	Datum a čas	Napadená organizace	Vzkaz útočníka oběti
				VARNSDORF - the world's leading machine-building plant engaged in the development, production, sale and service of machine tools
21.	pondělí	2023-01-16 10:23:00	ZETOR TRACTORS a.s.	The website of the ZETOR TRACTORS company, which specializes in the production and sale of tractors and engines, cannot rise after our DDoS attack
22.	pondělí	2023-01-16 10:31:00	AERO Vodochody AEROSPACE a.s.	AEROSPACE designs and manufactures military and civil aircraft and is the largest aircraft manufacturer in the Czech Republic. And we've killed their website
23.	úterý	2023-01-17 09:39:00	PILOUS - pásové pily, spol. s r.o.	We continue the Czech journey through the factories🇨🇿❌PILOUS - production of band saws for metal
24.	úterý	2023-01-17 09:40:00	Pásová ocel, s. r. o.	Due to our DDoS attack, the website of PÁSOVÁ OCEL, a company selling and processing strip steel, went to rest
25.	úterý	2023-01-17 09:42:00	Poldi Steel s.r.o.	The site of the metallurgical plant Poldi also could not resist DDoS attacks
26.	úterý	2023-01-17 09:43:00	EMP, s.r.o.	We've killed the website of the manufacturer of electric pumps and electric motors EMP
27.	úterý	2023-01-17 09:44:00	FERMAT CZ s.r.o.	A professional manufacturer of horizontal boring and point grinding machines LLC Fermat TsZ receives from us a portion of DDoS attacks on its main website
28.	úterý	2023-01-17 10:02:00	ReTOS Varnsdorf s.r.o.	The company RETOS Varnsdorf sro, which offers services for the operation of horizontal boring machines, falls under the weight of DDoS
29.	úterý	2023-01-17 10:21:00	KOVOSVIT MAS Machine Tools, a.s.	We've killed the website of a large Czech manufacturer of machine tools KOVOSVIT MAS Machine Tools
30.	středa	2023-01-18 10:24:00	Slovácké strojírny, a. s.	We kill the website of the machine tool manufacturer Slovácké strojírny as
31.	středa	2023-01-18 10:25:00	Ministerstvo obrany	The cybersecurity specialists of the Czech Ministry of Defense could not withstand the attack of the DDoS specialists from the NoName057(16) team
32.	středa	2023-01-18 10:38:00	Ministerstvo obrany	Following the main site, the site of the group of cybernetic forces and information operations went to recover😉
33.	středa	2023-01-18 11:03:00	Ministerstvo obrany	The digital office of the Ministry of Defense of the Czech Republic does not lag behind its comrades and falls under the onslaught of DDoS attacks
34.	středa	2023-01-18 12:01:00	Šmeral Brno, a.s.	The website of the Czech company Šmeral Brno as, which produces turnkey automated molding systems, went to recover after our DDoS attack
35.	středa	2023-01-18 12:30:00	Česká agentura na podporu obchodu	And now let's send "hello" to the Czech Ministry of Industry and Trade and its subdomains - firstly, we kill the main site
36.	středa	2023-01-18 13:02:00	Česká agentura na podporu obchodu	Another subdomain of the Ministry of Industry of the Czech Republic - the client zone - went offline
37.	středa	2023-01-18 13:30:00	Česká agentura na podporu obchodu	We've killed the portal of the official database of the Czech Ministry of Industry
38.	středa	2023-01-18 14:00:00	Česká agentura na podporu obchodu	The authorization service in the portal of the Czech trade promotion agency has sunk into oblivion
39.	středa	2023-01-18 14:31:00	Česká agentura na podporu obchodu	The portal of Czech trade missions also "lay down to rest" after our DDoS attack
40.	čtvrtek	2023-01-19 09:28:00	Ministerstvo financí	Today we have successfully killed the website of the Ministry of Finance of the Czech Republic
41.	čtvrtek	2023-01-19 11:40:00	JAWA Moto spol. s r. o.	Jawa Moto main site
42.	čtvrtek	2023-01-19 11:41:00	TAJMAC - ZPS a.s.	Killed the site of the Czech production program TAJMAC-ZPS
43.	čtvrtek	2023-01-19 11:42:00	Ministerstvo dopravy	The website of the Czech Ministry of Transport closed access to users from all countries except their own
44.	čtvrtek	2023-01-19 11:43:00	Ministerstvo dopravy	The subdomain of the Ministry of Transport - an authorization service - was closed from users, it works only in the Czech Republic
45.	čtvrtek	2023-01-19 11:50:00	Ministerstvo průmyslu a obchodu	Due to our DDoS attack, the website of the Czech Ministry of Industry feels "sick"
46.	pátek	2023-01-20 10:26:00	technology-support s.r.o.	We continue to punish the portals of the Russophobic Czech Republic🇨🇿❌Main website of T-Support, a supplier of industrial machine parts
47.	pátek	2023-01-20 11:09:00	Ministerstvo průmyslu a obchodu	The site of blockchain notary technology for civil servants and businessmen of the Czech Republic went to rest
48.	pátek	2023-01-20 11:45:00	EXCALIBUR ARMY spol. s r.o.	The website of the Czech company EXCALIBUR ARMY, which produces military equipment, was killed
49.	pátek	2023-01-20 12:30:00	TST servis a.s.	We kill the website of the company engaged in the supply of components for machine-building production "TST service"
50.	pátek	2023-01-20 13:14:00	ČKD GROUP, a.s.	We kill a subdomain of the website of the company CHKD GROUP - the login portal
51.	pátek	2023-01-20 14:02:00	TOS Varnsdorf a.s.	Due to our DDoS attack, the subdomain of the website of the Czech company TOS VARNSDORF, which develops, manufactures, sells and maintains machine tools, is not working
52.	sobota	2023-01-21 08:35:00	TOSHULIN, a.s.	The day begins with the punishment of the Czech manufacturer of lathes TOSHULIN - the main website is not working after our attack
53.	sobota	2023-01-21 09:13:00	TOS Svitavy, a.s.	We kill the website of the Czech metallurgical company Tos Svitavy
54.	sobota	2023-01-21 12:07:00	AERO Vodochody AEROSPACE a.s.	This is not the first time we kill the website of the Czech aircraft manufacturer AEROSPACE😉
55.	sobota	2023-01-21 13:21:00	Kovohutě Příbram nástupnická, a.s.	The website of the Czech metalworking plant Kovohutě Příbram was unable to process a bunch of requests and fell ill from a DDoS attack
56.	sobota	2023-01-21 14:32:00	Vanad 2000 a.s.	The website of the Czech supplier of high-performance machines "Vanad" does not withstand DDoS hail
57.	sobota	2023-01-21 15:10:00	WEILER Holoubkov s.r.o.	The website of the Czech company Weiler, which provides maintenance and overhaul of machines of a special production program, was closed from users after our DDoS attack😉
58.	sobota	2023-01-21 16:11:00	ALFE BRNO, s.r.o.	The portal of the Czech foundry ALFE BRNO received a DDoS hail and went to rest
59.	sobota	2023-01-21 16:47:00	Poldi Steel s.r.o.	The website of the Czech metallurgical plant Poldi does not get up after a DDoS attack😬
60.	neděle	2023-01-22 09:26:00	Ministerstvo obrany	Today we went on an exciting journey through the subdomains of the Czech Ministry of Defense🔥❌Website of the agency of communication and information systems
61.	neděle	2023-01-22 10:01:00	Ministerstvo obrany	The Czech computer incident response service portal, called "circus"😬, accepts our DDoS attack
62.	neděle	2023-01-22 10:45:00	Ministerstvo obrany	The open data portal of the Ministry of Defense of the Czech Republic became an inaccessible data portal after our DDoS attack😉
63.	neděle	2023-01-22 11:30:00	Ministerstvo obrany	The main website of the Czech Ministry of Defense cowardly closed from users of all countries except

P. č.	Den	Datum a čas	Napadená organizace	Vzkaz útočníka oběti
				the Czech Republic😂
64.	neděle	2023-01-22 12:25:00	Ministerstvo obrany	The Czech Ministry of Defense restricted access to another portal after our attack - the site for the development of military research
65.	neděle	2023-01-22 14:16:00	Ministerstvo obrany	The website of the 24th transport aviation base, a subdomain of the portal of the Ministry of Education of the Czech Republic, also closes access after our DDoS attack
66.	neděle	2023-01-22 14:36:00	Ministerstvo obrany	Another subdomain of the website of the Ministry of Defense of the Czech Republic - the website of the Pardubice Airport Administration - was closed after non-flying weather due to DDoS hail:
67.	neděle	2023-01-22 15:11:00	Ministerstvo obrany	Another subdomain of the Czech Ministry of Defense was forced to close - the army portal
68.	neděle	2023-01-22 15:50:00	Ministerstvo obrany	Another subdomain of the main website of the Czech Ministry of Defense became inaccessible after DDoS
69.	pondělí	2023-01-23 15:03:00	Avast Software s.r.o.	Well... You obviously remember how Avast spoke about our activities and how its "experts" told us that we supposedly have a low intensity of DDoS attacks
70.	pondělí	2023-01-23 15:52:00	Avast Software s.r.o.	By the way! Do you know what are the passwords of some accounts of Avast employees?😈 Here they are: ""viewsonic 17gs", "3518754", ""time for rock"
71.	pondělí	2023-01-23 15:53:00	Avast Software s.r.o.	"Avast", stop changing servers, we see everything and follow your brown trail😈
72.	pondělí	2023-01-23 15:56:00	Avast Software s.r.o.	Do you know that Avast temporarily suspended activities on the territory of Russia🇷🇺? The reason: the ban on the supply of high-tech solutions.
73.	pondělí	2023-01-23 15:59:00	Avast Software s.r.o.	Do you know, friends, that "Avast" once was caught selling user data, including residents of our country🇷🇺?🤬The best thing that can help them is a lobotomy procedure. Although... can someone start selling their employees' data from their corporate network?😉 We think this is a fair deal😈
74.	pondělí	2023-01-23 16:04:00	Avast Software s.r.o.	Art motifs for today's attack on Avast😂
75.	pondělí	2023-01-23 16:34:00	Avast Software s.r.o.	Time is running, Avast's resources are lying after our attack, the number of questions to the Czech IT company is increasing, people are complaining about problems, and Avast itself has activated the "Pretend to be a hose" mode and is silent, as if it has filled its mouth with water...😂
76.	úterý	2023-01-24 20:20:00	Avast Software s.r.o.	After our DDoS attack yesterday Avast only had enough strength to raise its forum only in Bulgaria!!! Circus, not an IT company 🤡 🤣
77.	úterý	2023-01-24 20:22:00	Workday, Inc.	We continue our trip to Avast and we do not let the HR portal of Czech IT specialists, which fell yesterday, rise😂
78.	pátek	2023-01-27 09:11:00	Pro bezpečnou budoucnost z.s.	We haven't forgotten about the second round of elections in the Czech Republic😉 The site of the candidate Peter Pavel was shut down again🪄
79.	pátek	2023-01-27 09:50:00	Ministerstvo zahraničních věcí	The website of the Czech Ministry of Foreign Affairs goes offline
80.	pátek	2023-01-27 10:26:00	Hlídač státu, z.ú.	Again, the Czech "State Watchman" sleeps at his workplace after a DDoS attack:
81.	sobota	2023-01-28 09:50:00	Pro bezpečnou budoucnost z.s.	And we continue to closely monitor the presidential elections in the Czech Republic🇨🇿 and report to you the situation in this Russophobic country😉 The website of one of the candidates, Petr Pavel, who is known for his anti-Russian statements, is down again
82.	sobota	2023-01-28 09:50:00	Pro bezpečnou budoucnost z.s.	And we continue to closely monitor the presidential elections in the Czech Republic🇨🇿 and report to you the situation in this Russophobic country😉 The website of one of the candidates, Petr Pavel, who is known for his anti-Russian statements, is down again
83.	sobota	2023-01-28 10:20:00	Český statistický úřad	What are the statistics of the candidates for the presidency of the Czech Republic? And we also do not know, because we shut down their statistical portal with the voting results
84.	sobota	2023-01-28 13:10:00	Ministerstvo zahraničních věcí	Access to the portal of the Czech Ministry of Foreign Affairs is now only available to foreigners due to our DDoS attack - the portal does not work for Czechs😀
85.	neděle	2023-01-29 13:30:00	Český statistický úřad	And how are the things going in the Czech Republic🇨🇿? The elections are over, the president has changed. Only the sphere of information security does not change: the portals continue to feel sick: ❌Statistical Information Service of the Czech Statistical Office
86.	čtvrtek	2023-02-02 13:15:00	M E L M A R K s.r.o.	Today, in Sergey Karnaukhov's Telegram channel, we saw a post about a Russophobic bar in the Czech Republic, where someone decided to rename the "White Russian" cocktail to "Dead Russian"🤬In short, we could not pass by and crashed the site of this eatery

Zdroj: Telegram, CZECHMATE CZ s.r.o.