Jak USA ohrožují globální internetovou bezpečnost desetiletími kybernetického sledování, útoků

globaltimes.cn/page/202305/1290553.shtml

DO HLOUBKY / DO HLOUBKY
Jak USA ohrožují globální internetovou bezpečnost desetiletími kybernetického sledování, útoků

Říše dohledu

Reportéři štábu GTZveřejněno: 11. května 2023 20:22
Aktualizováno: 12. května 2023 00:01

Foto: VCG

Poznámka editora:

Uplynulo deset let od chvíle, kdy Edward Snowden odhalil skandál PRISM a rozzuřil svět. Pod rouškou takzvaných „národních zájmů“ využívá americká vláda a její spřízněné zpravodajské agentury své

technologické a prvotřídní výhody k provádění kybernetického sledování a útoků po celém světě.

Dokumenty, které unikly z Pentagonu začátkem tohoto roku, nabídly další důkaz, že USA natáhly ruku téměř do všech koutů světa. Jaké zlé skutky USA zorganizovaly a pravděpodobně pokračují v kybernetickém světě? V této sérii se Global Times podrobně zaměří na to, jak toto skutečné „impérium sledování sítě“ postupně poškozuje globální kybernetickou bezpečnost prostřednictvím své zpravodajské sítě.
Nedávno uniklé dokumenty Pentagonu znovu odhalily světu ošklivou tvář amerických špionážních kampaní organizovaných proti jiným zemím. Zatímco udržují přísný dohled nad svými „nepřáteli“ i spojenci, natáhly USA svou zlou ruku téměř do všech koutů světa.

Spojené státy léta prováděly rozsáhlé sledování a spouštěly kybernetické útoky zaměřené na zámořské vlády, společnosti a jednotlivce s technologickými výhodami a rozsáhlou zpravodajskou sítí, což je vážné porušení mezinárodního práva a základních norem upravujících mezinárodní vztahy. A co je ještě horší, USA se při páchání těchto ničemných činů vykreslují jako oběť tím, že hanobí ostatní země včetně Číny nepodloženými obviněními.

Minulý měsíc vydala čínská organizace Cybersecurity Industry Alliance (CCIA) zprávu s názvem „Přehled kybernetických útoků od amerických zpravodajských agentur – na základě analýz globálních komunit kybernetické bezpečnosti“.

Zpráva podrobně popisuje zlomyslné chování USA při provádění dlouhodobých kybernetických útoků a sledování po celém světě, jako jsou útoky proti klíčové infrastruktuře v jiných zemích, nerozlišující kybernetické krádeže a monitorování a zavádění standardů znečištění zadních vrátek a zdrojů dodavatelského řetězce.

Zpráva předkládá důkazy, které odhalují skutečnou povahu role USA jako největšího světového zloděje tajných informací a „hackerského impéria," Qin An, zástupce ředitele expertního výboru pro boj proti terorismu a řízení kybernetické bezpečnosti, Čínská policejní společnost. Zákon,

Chování Spojených států značně poškodilo pořádek v kyberprostoru a zničilo již tak křehkou důvěru mezi zeměmi, komentoval Tang Lan, ředitel Centra pro studium kyberprostorové bezpečnosti a správy v China Institutes of Contemporary International Relations.

"Jeho zlé činy přidaly mezinárodní situaci mnoho nejistoty," řekl Tang pro Global Times.

Špinavá historie

V září 2022 odhalilo čínské Národní centrum pro nouzovou reakci na počítačové viry dlouhodobý kybernetický útok USA proti Severozápadní polytechnické univerzitě (NPU) v provincii Shaanxi v severozápadní Číně. Kybernetický útok byl zaměřen na „infiltraci a kontrolu základního vybavení v čínské infrastruktuře a na krádež citlivých osobních údajů vázaných na Číňany," řekl tehdy pro Global Times zdroj blízký této záležitosti.

To byla jen špička ledovce. Již více než deset let Spojené státy monitorují 45 zemí a regionů prostřednictvím pokročilého a skrytého „telescreenu" (Bvp47), který vytvořila Equation, elitní hackerská skupina přidružená k americké vládě. Když to čínští odborníci na kybernetickou bezpečnost poprvé odhalili na začátku roku 2022, vyvolalo celosvětové pobouření.

Tento incident veřejnosti připomněl známější PRISM, protože výzkumníci našli několik programů a příruček k útokům, které při kontrole odpovídaly jedinečným identifikátorům používaným v operačních příručkách platforem pro kybernetické útoky v rámci americké Národní bezpečnostní agentury (NSA). Ten byl odhalen

bývalým analytikem Ústřední zpravodajské služby (CIA) Edwardem Snowdenem v roce 2013 jako malá část tehdejšího mezinárodního skandálu PRSIM.

V červnu 2013 se The Guardian stal jedním z prvních médií, které informovaly o tajném programu USA s kódovým názvem „PRISM“, který Snowden odhalil. Exposé odhalilo, že devět amerických internetových gigantů, včetně Microsoft, Yahoo, Google a Apple, spolupracovalo s americkou vládou na tajném sledování telefonních záznamů, e-mailů, videí a fotografií a NSA se dokonce nabourala do sítí několika zemí, jako je Německo a Jižní Korea.

"Následná série uniklých dokumentů společně odhalila, že operace monitorování a narušení sítě byly prováděny americkou vládou po dlouhou dobu," poznamenala zpráva CCIA.

Později, v červnu 2015, Snowden odhalil dokumenty odhalující, jak zpravodajské agentury v USA a Spojeném království spolupracovaly na podvracení antivirového a jiného bezpečnostního softwaru za účelem sledování uživatelů a infiltrace sítí. Pobuřující projekt, pojmenovaný CAMBERDADA, využíval především schopnosti USA získávat provoz při invazi globálních operátorů k monitorování komunikace mezi uživateli a antivirovými společnostmi, jako je Skyscraper v Rusku, k získávání nových vzorků virů a dalších forem informací, uvedla zpráva CCIA.

Podle článku zveřejněného na zpravodajském webu The Intercept ten měsíc, uniklá prezentace z roku 2010 o "Projektu CAMBERDADA" uvádí 23 dalších antivirových společností z celého světa pod "Další cíle!" Čínská Antiy byla na seznamu.

Odhalení opět vyvolalo široké pobouření, protože pozorovatelé varovali, že projekt a jeho takzvaný „seznam cílů“ dále rozdělí již tak roztřepený globální bezpečnostní průmysl.

Je těžké přesně sledovat, jak USA začaly své nečestné kybernetické kampaně. Počítačový červ „Stuxnet“, kterého americké zpravodajské služby použily při útoku na íránská jaderná zařízení v roce 2010, byl průmyslem kybernetické bezpečnosti považován za „první kybernetickou zbraň na světě“.

Vývoj viru Stuxnet údajně začal v roce 2005. V roce 2010 Stuxnet údajně „zničil téměř pětinu íránských jaderných odstředivek, infikoval přes 200 000 počítačů a způsobil fyzickou degradaci 1 000 strojů“, uvádí data, která Kaspersky sdílel na svých webových stránkách.

Toho roku USA „otevřely Pandořinu skříňku kybernetické války,“ komentovala zprávu CCIA.

Bývalý francouzský premiér Francois Fillon na slyšení 2. května 2023 odhalil, že americká Národní bezpečnostní agentura v letech 2007 až 2012 špehovala jeho rozhovory s bývalým francouzským prezidentem Nicolasem Sarkozym. Foto: IC

Rozsáhlá sledovací síť

Podle dubnové zprávy jednoho amerického média utratí americké zpravodajské agentury za rok až 90 miliard dolarů. Za rozsáhlou sledovací sítí v USA stojí zpravodajské agentury jako NSA a CIA, které opakovaně uváděly národní bezpečnost jako záminku k porušování suverenity jiných zemí a narušování soukromí jejich občanů.

Úřad of Tailored Access Operation (TAO) pod NSA, který byl zapojen do akce NPU, provádí útoky proti Číně pronikáním do čínských počítačových a telekomunikačních systémů po celá desetiletí.

TAO byla založena v roce 1998 a v současnosti je taktickou implementační jednotkou v rámci vlády USA, která se specializuje na rozsáhlé síťové hackování a špionáž proti jiným zemím. Skládá se z více než 2 000 vojenských a civilních pracovníků, podle společné technické analýzy a sledování vyšetřování provedeného National Computer Virus Emergency Response Center a 360 Security Technology v září 2022.

Poslání TAO je jednoduché – „shromažďuje zpravodajské informace o cizích cílech tajným pronikáním do jejich počítačů a telekomunikačních systémů, prolomením hesel, kompromitováním počítačových bezpečnostních systémů chránících cílový počítač, krádeží dat uložených na pevných discích počítačů a následným zkopírováním všech zprávy a datový provoz procházející v rámci cílených systémů elektronické pošty a textových zpráv," uvádí Foreign Policy s odkazem na bývalého úředníka NSA Matthewa M. Aida.

USA použily 41 druhů vyhrazených zbraní pro kybernetické útoky k zahájení tisíců útoků ve snaze ukrást základní technologická data z NPU. Kromě toho se USA již dlouho zabývají nevybíravým hlasovým

monitorováním čínských uživatelů mobilních telefonů, nelegálním přístupem k textovým zprávám a prováděním bezdrátového sledování polohy.

Kromě kybernetických útoků na Čínu je známý i konflikt mezi USA a Ruskem v oblasti kybernetické bezpečnosti. Podle zpráv generál Paul Nakasone, šéf NSA, potvrdil, že američtí vojenští hackeři provedli kybernetické útoky proti Rusku na podporu Ukrajiny.

Již nějakou dobu se USA ve jménu budování kapacit snaží přimět příslušné země, zejména sousedy Číny, aby s nimi spolupracovaly v oblasti kybernetické bezpečnosti. Prosazuje dokonce takzvané „Forward Deployment“ kybernetických vojenských sil. "Otevře taková spolupráce zadní vrátka pro zákeřné kybernetické aktivity USA? Stanou se takové kroky šachovými figurkami, protože USA podněcují geostrategickou rivalitu? Příslušné země posoudí samy," řekl Wang Wenbin, mluvčí čínského ministerstva zahraničí. Global Times dne 20. dubna 2022 v reakci na to, že National Computer Virus Emergency Response Center upozornilo země na kybernetické útoky prováděné vládou USA.

Internetová bandita

Skandály jako PRISM ukázaly, že kromě svých zpravodajských agentur je mnoho internetových podniků také nuceno nebo oklamáno vládou USA, aby rozšířily svou síť kybernetického dohledu a útoků.

Aby sloužily svému shromažďování zpravodajských informací a vývoji kybernetických zbraní, USA údajně instalovaly zadní vrátka do různých hardwarových a softwarových produktů, což není nic jiného než naprostý banditismus, odsuzovali experti na kybernetickou bezpečnost oslovení Global Times.

Například média v únoru 2020 odhalila, že CIA a německá Federální zpravodajská služba (BND) byly schopny číst šifrovanou komunikaci od Crypto AG, švýcarské společnosti, která vyráběla šifrovací systémy pro mnoho vlád, společným přidáním zadních vrátek do šifrovacích produktů Crypto AG.

Podle zprávy CIA zmíněné v článku Washington Post z 11. února 2020 byla operace nazvána „zpravodajským převratem století“.

Qin řekl, že pomocí své řídící pravomoci internetu americké zpravodajské agentury navrhly speciální zadní vrátka a vložily je do produktů, které byly předtím předloženy CIA k rutinní kontrole, než byly schváleny pro export, a poskytly tak přímý přístup do sítí jiných zemí. Pro podniky v jiných zemích se proto stává riskantní používat produkty vyvinuté americkými subjekty.

"S úpadkem americké hegemonie v reálném prostoru bude země podnikat odvážnější kroky v kyberprostoru," předpověděl Qin.

Ve snaze dále pomlouvat další země včetně Číny přidalo 22. května 2020 americké ministerstvo obchodu na svůj seznam subjektů 33 čínských společností, z nichž většina jsou společnosti zaměřující se na technologii AI a jsou poskytovateli služeb síťové komunikace, jako např. Qihoo 360 a Cloudminds, tvrdí, že tyto společnosti by mohly ohrozit americkou národní bezpečnost a zahraniční politiku.

Experti blízcí čínské síťové komunikaci a bezpečnosti kyberprostoru, kterých se dotkl Global Times, však uvedli, že tyto čínské společnosti nešpehují jiné země ani nemají schopnost vkládat zadní vrátka do kyberprostoru USA.

Chování USA spočívající v zařazení některých čínských technologických společností na svůj seznam subjektů je typickým případem technologické šikany, řekl Qin.

Všechny tyto skutečnosti opakovaně odhalily pravou tvář USA jako šikanující síly a odhalily, kdo je zodpovědný za nejistotu a nestabilitu v kyberprostoru, upozornil Tang.

SOUVISEJÍCÍ ČLÁNKY

„Tyranie“ protičínských státních zákonů ještě více ztěžuje zvrácení čínsko-amerických vazeb

Uprostřed napjatých čínsko-amerických vztahů američtí politici nadále přilévají olej do ohně schvalováním protičínských zákonů,...

NEJSLEDOVANĚJŠÍ