Attacking Empire: Jak USA ohrožují globální bezpečnost bezohlednými kyberútoky a rozsáhlým arzenálem kybernetických zbraní

globaltimes.cn/page/202306/1291786.shtml

DO HLOUBKY / DO HLOUBKY

Útočící impérium: Jak USA ohrožují globální bezpečnost bezohlednými kybernetickými útoky a rozsáhlým arzenálem kybernetických zbraní

Jak USA ohrožují globální bezpečnost bezohlednými kybernetickými útoky a rozsáhlým arzenálem kybernetických zbraní

Reportéři štábu GTZveřejněno: 1. června 2023 20:30 Aktualizováno: 1. června 2023 20:50

-
-
-
-
-

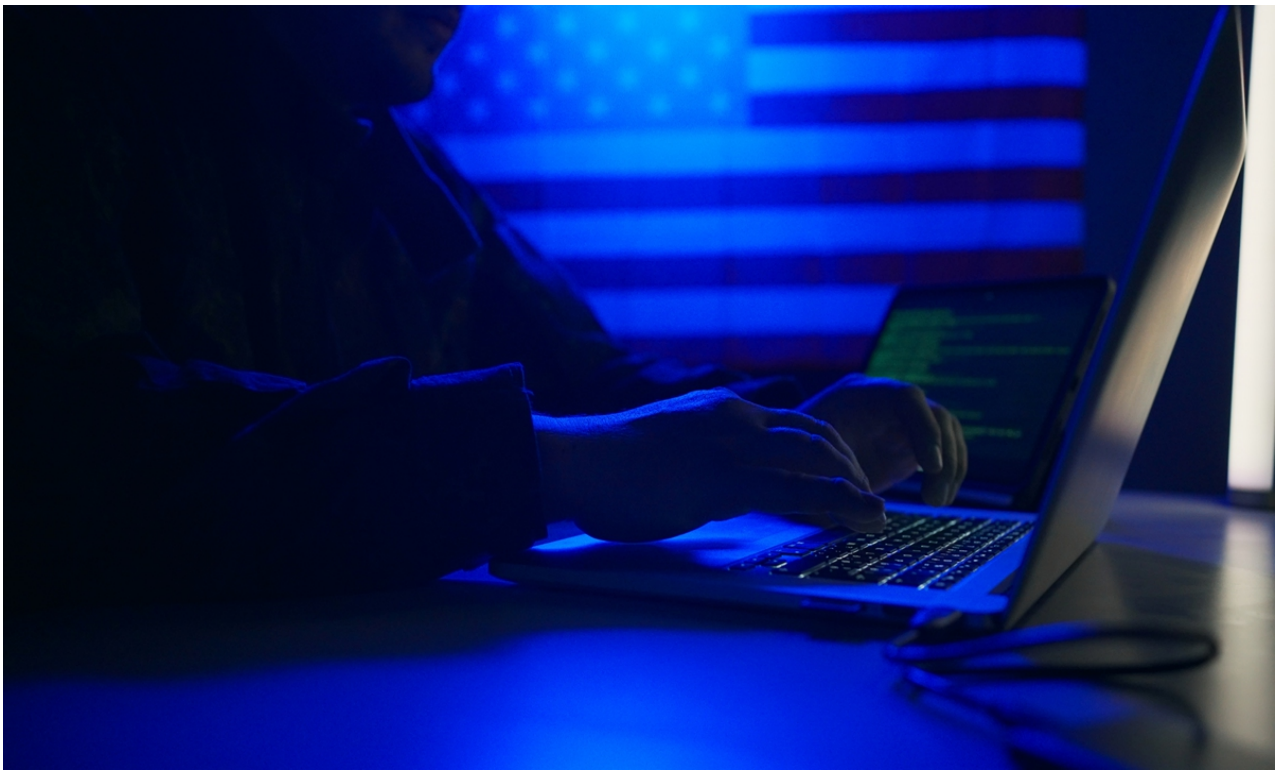

Foto: VCG

Poznámka editora:

Uplynulo deset let od chvíle, kdy Edward Snowden odhalil skandál PRISM, který rozzuřil svět. Pod rouškou takzvaných národních zájmů americká vláda a její spřízněné zpravodajské agentury využívají svých technologických výhod a výhod prvního tahu k provádění kybernetického sledování a útoků na zbytek světa.

Spojené státy se spoléhají na svou hegemonii v kyberprostoru a používají kybernetické schopnosti jako jeden ze svých nástrojů v hybridní válce. Stejně jako jiné nástroje, jako jsou ekonomické sankce, teroristické aktivity a vojenská intervence, použily USA kybernetickou válku k zasahování do vnitřních záležitostí jiných zemí ak dosažení svých vlastních politických cílů. Aby si udržely svou hegemonii, provedly USA „digitální kolonizaci“ nad jinými zeměmi a spáchaly různé zločiny konvertitů, čímž se staly „říší dozoru“, „říší útoků“ a „říší šikany“.

Ve třetím pokračování této série se Global Times zabývá tím, jak toto „útočné impérium“ kazí kyberprostor a ohrožuje globální bezpečnost častými kybernetickými útoky, a co se skrývá uvnitř obrovského arzenálu amerických kybernetických zbraní.

I když se USA nikdy nesnažily skrývat své intriky přilévání oleje do ohně rusko-ukrajinského konfliktu, USA znovu ukázaly světu své různé hrozné prostředky kybernetických útoků proti Rusku i proti více zemím a regionům po celém světě. Šéf amerického kybernetického velení médiím přiznal, že američtí vojenští hackeři provedli útočné operace zaměřené na Rusko „na podporu Ukrajiny“.

Od široce známého skandálu PRISM, který odhalil spoustu špinavých triků, které USA provedly v kybernetickém světě, je toto největší impérium kybernetických útoků stínem vznášejícím se nad lidmi z celého světa se svými četnými ničivými kybernetickými

zbraněmi, které mohou a pravděpodobně mají, způsobily velké škody na cílech z klíčových průmyslových odvětví po každý aspekt každodenního života.

"USA jsou zakladatelem internetu a iniciátorem kybernetické války," řekl Qin An, zástupce ředitele expertního výboru pro boj proti terorismu a řízení kybernetické bezpečnosti, Čínské společnosti pro policejní právo. "USA byly první, kdo otevřel cestu k paralyzaci a zničení skutečného světa z kyberprostoru."

Bez skrupulí v kybernetickém světě

Investigativní zpráva, kterou minulý měsíc společně zveřejnilo čínské Národní středisko pro nouzovou reakci na počítačové viry (CVERC) a společnost 360 pro internetovou bezpečnost, odhalila případy, kdy americká Ústřední zpravodajská služba (CIA) použila síť k útoku na Čínu a další země. Poskytla další důkazy ukazující dlouhodobé bezohledné kybernetické útoky USA, které vytvořily chaos a zmatek po celém světě.

Po desetiletích se USA údajně pokoušely svrhnout legitimní vlády prostřednictvím „barevných revolucí“ ve více než 50 zemích. Rozvoj internetu na začátku 21. století umožnil CIA provádět infiltrativní, podvratné a sabotážní aktivity rychlejšími a skrytějšími metodami s pomocí některých amerických technologických společností, uvádí zpráva.

Například „rojení“ byla netradiční technika změny režimu vyvinutá americkou RAND Corporation jako nástroj pro komunikaci na místě pro demonstrace založené na internetu a bezdrátové komunikaci. Tato technika byla použita k „postrčení mladých lidí připojených přes internet, aby se připojili k protestům proti plynulosti 'jeden výstřel pro jiné místo'“ během „barevných revolucí“ vyvolaných CIA.

Jako hlavní imaginární nepřítel bylo Rusko hlavním cílem kybernetických útoků USA, zejména během probíhající rusko-ukrajinské krize. Generál Paul Nakasone, šéf amerického Cyber Command, potvrdil Sky News, že USA provádějí útočné hackerské operace na podporu Ukrajiny.

"Provedli jsme řadu operací napříč celým spektrem; útočné, obranné a informační operace," řekl Nakasone. Vysvětlil, že kybernetické útoky zaměřené na Rusko byly zákonné a vedené na základě politiky, o které rozhodlo americké ministerstvo obrany, uvedla Sky News v červnu 2022.

Do května 2022 se více než 65 000 hackerů z několika západních zemí včetně USA pravidelně účastnilo DDoS útoků proti ruské „kritické informační infrastruktuře“, řekl v červnu téhož roku mluvčí ruského ministerstva zahraničí Alexander Krutskikh.

Čína je také hlavní obětí bezohledných kybernetických útoků USA. Podle zprávy vydané CVERC v roce 2021 Čína v roce 2020 zachytila přes 42 milionů vzorků škodlivých programů. Ty pocházející z USA představovaly 53,1 procenta všech vzorků pocházejících ze zámoří.

V září 2022 CVERC odhalil dlouhodobé kybernetické útoky USA proti Severozápadní polytechnické univerzitě (NPU) v provincii Shaanxi v severozápadní Číně, které měly kontrolovat infrastrukturní vybavení a krást osobní informace, což je jeden z nedávných důkazů, které ukazují, že USA se protáhly. natáhnout své zlé ruce na obyčejné čínské lidi.

Ani mnozí „spojenci“ USA nejsou schopni kybernetické útoky přežít. V roce 2022 odborníci na kybernetickou bezpečnost z laboratoře Qi An Pangu se sídlem v Pekingu pro Global Times sdělili, že objevili špičkovou hackerskou skupinu v rámci americké Národní

bezpečnostní agentury (NSA), která používá kybernetickou zbraň s názvem „Telescreen“ již déle než desetiletí infiltrovat a zaútočit na 45 zemí a regionů, zahrnujících 287 důležitých institucionálních cílů.

Kromě Číny a Ruska byly na seznamu také proamerické země včetně Japonska, Německa a Itálie.

Jak děsivě všeprostupující je americká síť kybernetických útoků? Odpověď lze nalézt dříve v roce 2017, kdy WikiLeaks odhalila 8 761 dokumentů od CIA, které podrobně popsaly nástroje, které používala k nabourání se do telefonů, komunikačních aplikací a dalších běžně používaných elektronických zařízení používaných v každodenním životě.

"Útočný systém CIA nazvaný Fine Dining poskytuje 24 návnadových aplikací pro špiony CIA," uvedl The Guardian s odkazem na WikiLeaks v článku zveřejněném v březnu téhož roku.

"Svědkům se zdá, že špión spouští program, který zobrazuje videa, prezentuje diapozitivy, hraje počítačovou hru nebo dokonce spouští falešný antivirový skener," uvedl The Guardian. "Ale zatímco je návnada aplikace na obrazovce, systém je automaticky infikován a vypleněn."

"USA jsou jedinou zemí na světě, která prosazuje útočnou strategii v oblasti kyberprostoru. Často provádí kybernetické útoky a 'sankce' proti jiným zemím pomocí svých kybernetických zbraní," řekl Fang Xingdong, zakladatel technologického think-tanku ChinaLabs se sídlem v Pekingu. Global Times ve středu.

Fang poznamenal, že národní zájmy USA vstupují do základní logiky útočného chování americké vlády. "Když USA provádějí kybernetické útoky, jejich sledování zájmů často vede k tomu, že nerozlišují mezi svými spojenci a nespojenci," řekl Fang.

Ofenzivní strategie USA se podle něj stala klíčovým faktorem způsobujícím nestabilitu v globálním kyberprostoru.

Surveillance Empire: Spying for profit Grafika: GT

Nekontrolovatelná nebezpečí pro životy lidí

Spojené státy mají impozantní kybernetickou sílu schopnou ohrozit každou oblast každodenního života od zdravotnických systémů po vodu a elektřinu kybernetickými útoky, které by mohly ostatní země snadno srazit na kolena, citovala agentura Xinhua tureckého bezpečnostního specialistu Ismaila Hakkiho. Pekin, jak se říká v dubnu.

Ransomwarový útok WannaCry v roce 2017 například ukázal světu, jak mohou americké kybernetické zbraně způsobit nekontrolovatelné nebezpečí pro životy lidí.

Ransomware, který se rozšířil po celém světě v květnu 2017, zasáhl více než 300 000 počítačů ve 150 zemích a regionech a 100 000 organizací, což mělo za následek celkovou ztrátu přibližně 50 miliard juanů (7,04 miliardy dolarů). Bylo napadeno mnoho nemocnic, vzdělávacích institucí a vládních úřadů.

Hlavním důvodem, který vedl k šíření ransomwaru WannaCry, byla kybernetická zbraň Eternal Blue, kterou vyvinula NSA. Všeobecně se věřilo, že únik Eternal Blue umožnil WannaCry řádit pod kontrolou hackerů.

Roky po skandálu PRISM nehoda Eternal Blue lidem znovu připomněla obrovský arzenál kybernetických zbraní USA, který byl pravděpodobně zodpovědný za mnoho kybernetických katastrof na celém světě. NSA zahájila kybernetické útoky proti 47 zemím a regionům už deset let, řekl exkluzivně v březnu Global Times odborník na kybernetickou bezpečnost z 360.

V desetiletých útocích byly použity různé kybernetické zbraně, včetně backdoor programu UnitedRake, útočného systému QUANTUM a falešného serveru FOXCID. FOXCID je výkonný „nástroj pro invazi ve velkém měřítku“, platforma pro útoky na zranitelnost, která umožňuje operátorům s malými zkušenostmi účastnit se kybernetických útoků.

Je těžké přesně vědět, kolik kybernetických zbraní má NSA. Podle společnosti Kaspersky zabývající se kybernetickou bezpečností, která v roce 2015 odhalila, že 500 infekcí NSA „Equation Group“ v nejméně 42 zemích, byl malware Regin, škodlivé PHP skripty a počítačoví červi jako Fanny a Stuxnet některými z běžně používaných kybernetických útoků NSA. zbraně.

V roce 2010 infikovaly americké zpravodajské agentury pomocí Stuxnet více než 20 000 počítačů v Íránu a způsobily 1,

"Stuxnet přinesl velkou hrozbu pro lidskou společnost a i dnes zůstává hlubinnou bombou ohrožující bezpečnost světa," řekl Qin pro Global Times.

Výše zmíněné zbraně jsou jen špičkou ledovce obrovského arzenálu kybernetických zbraní NSA, nemluvě o dalších amerických ministerstvech včetně CIA a armády, které také vyvíjejí své vlastní kybernetické zbraně.

Podle Wikileaks do konce roku 2016 Centrum pro kybernetickou inteligenci (hackerská divize) spadající pod samotnou CIA naverbovalo přes 5 000 hackerů, kteří produkovali více než 1 000 malwarových systémů – virů, trojských koní a dalšího softwaru, který může proniknout ovládání cílové elektroniky.

Je obzvláště alarmující, že USA se svými technologickými výhodami a převahou v odvětví internetové infrastruktury pokračují ve vývoji řady kybernetických zbraní, které spustily nové kolo závodů ve zbrojení v kyberprostoru a přinesly nepředvídatelná rizika v globální kybernetické bezpečnosti, varovali pozorovatelé.

"Útoky ransomwaru po celém světě v posledních letech byly způsobeny hlavně únikem arzenálu kybernetických zbraní NSA. Únik dává mnoha jednotlivcům možnost provádět sofistikované vydírání a útoky. Tento efekt přelévání a nerozlišující globální sledování vážně nahlodaly základy důvěry mezi národy v digitálním věku,“

poznamenal Fang. "A nedostatek důvěry v digitální svět se stal jedním z největších světových problémů."