

Stuxnet

Digitální zbraň

Ondřej Tichý

4. února 2026

1 Historie

1.1 Vznik

Vše začalo v roce 2006 během volebního období prezidenta Spojených států amerických George W. Bushe. V Íránu (kde v této době vedli válku s USA) vzniklo nové zařízení pro obohacování uranu v Natanzu, pod záminkou energetické pomoci íránskému obyvatelstvu. Vláda USA si však uvědomovala, že tento uran by se dal využít i jako část nukleárních zbraní, a právě proto vznikla nová operace "Olympic Games" s cílem narušit toto zařízení [1].

První návrhy měly formu přímého útoku nebo sabotáže, ty však byly příliš neefektivní nebo nebezpečné. Prezident Bush byl zoufalý, proto povolil nápad generála J. E. Cartwrighta, velitele malého týmu pro kyberoperace.

Tento návrh byl ve své podstatě jednoduchý: získat kontrolu nad počítači v tomto zařízení. Prvním krokem bylo vypustit do systému "maják", který vytvoří elektronický plán celého zařízení. Tyto informace pak pošle přímo NSA (National Security Agency), kde podle nich vytvoří efektivní plán, jak převzít kontrolu nad celým systémem.

Po několika měsících se "majáky" ozvaly a poslaly kompletní plány zařízení. NSA se za pomoci spojenecké izraelské jednotky pustila do vývoje skutečného "červa", který zaútočí. Brzy vznikl program s jednoduchým názvem "the bug", potřebovali však ještě provést testy.

1.2 Průběh

S absolutní tajností USA postavilo repliky P-1 centrifug, zastaralé modely, jež byly využívány íránskou vládou. Začali malými testy, které byly až překvapivě úspěšné. "The Bug" napadl systém ovládající centrifugu, pobyl zde pár dní až týdnů, než poslal příkaz pro malou změnu rychlosti centrifug, což vedlo k jejich sebezničení. Úspěch přišel i u větších testů, a tím pádem bylo uděleno povolení k aktivnímu využití.



Obrázek 1: Model centrifugy P-1

Tento moment by se dal nazvat překročením Rubikonu, neboť to je první využití kybernetické zbraně k hmotné destrukci [2].

Dostat vir samotný do zařízení je však těžší než pouze "maják", ale má své metody. Jejich hlavní způsob stál na lidské nebezpečnosti. Jednoduše dali virus na USB flash disk a počkali, až ho nebezpečný zaměstnanec s přístupem k počítačům vloží. Samozřejmě později objevili lepší způsoby.

V roce 2008 začaly časté poruchy centrifug a íránské vedení bylo zmatené. "The Bug" byl naprogramovaný tak, aby dva útoky nevypadaly stejně, a navíc pro oklamání nepřítele posílal chybné informace kontrolorům provozu. Technici se snažili najít chybu, ale nenašli nic, což vedlo nejen k propuštění mnoha zaměstnanců, ale dokonce i k dočasnému uzavření určitých sektorů.

Po nástupu Baracka Obamy do funkce operace Olympic Games pokračovala. V roce 2010 však došlo k nečekanému vývoji. Napojení infikovaného počítače k celosvětové síti vedlo k rozšíření viru po celém světě a tím pádem k jeho odhalení. Naštěstí nemohl mít velký efekt vzhledem k jeho úzké specializaci. Vláda USA musela podstoupit potřebné kroky k uklidnění situace, přesto operace dále úspěšně pokračovala.

```
if ( LOBYTE(w2->UseShell32) )
{
    hShell32 = (w2->Data1.Api.CreateFileW)(w2->shell32_dll_path, -2147483648, 1, 0, 3, 0, 0); // open shell32.dll image
    BaseAddress = hShell32;
    if ( hShell32 == -1 )
        return -65530;
    Shell32 = (w2->Data1.Api.CreateFileMappingW)(hShell32, 0, 0x1000002u, 0, Size, 0); // create corresponding mapping
    (w2->Data1.Api.CloseHandle)(BaseAddress);
    if ( !hShell32 )
        return -65529;
    BaseAddress = (w2->Data1.Api.MapViewOfFile)(Shell32, 4, 0, 0, Size); // map view of file
    (w2->Data1.Api.CloseHandle)(Shell32);
}
else
{
    BaseAddress = (w2->Data1.Api.VirtualAlloc)(0, pInjectPe->OptionalHeader.SizeOfImage, 4096, 4);
}
if ( !BaseAddress )
    return 0xFFFF0000u;
if ( !(w2->Data1.Api.VirtualProtect)(BaseAddress, Size, PAGE_READWRITE, &w40) ) // change page protection
{
    w51 = 0xFFFF0000u;
    goto LABEL_109;
}
(w2->Data1.Apimemset)(BaseAddress, 0, pInjectPe->OptionalHeader.SizeOfImage); // zero memory
(w2->Data1.Api_memcpy)(
    BaseAddress,
```

Obrázek 2: Příklad kódu Stuxnet

1.3 Současnost

V této době už není Stuxnet aktivní hrozbou a údajně se sám zničil v roce 2012. Současně se na něj hlavně odkazuje jako na začátek "kybernetické války" (cybernetic warfare) a kam jsme se od té doby posunuli. Příklady virů, které inspiroval můžou například být Duqu, Flame, nebo Industroyer.

Reference

- [1] David E. Sanger. Obama order sped up wave of cyberattacks against iran. *The New York Times*, June 2012.
- [2] Kim Zetter. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown, 2014.