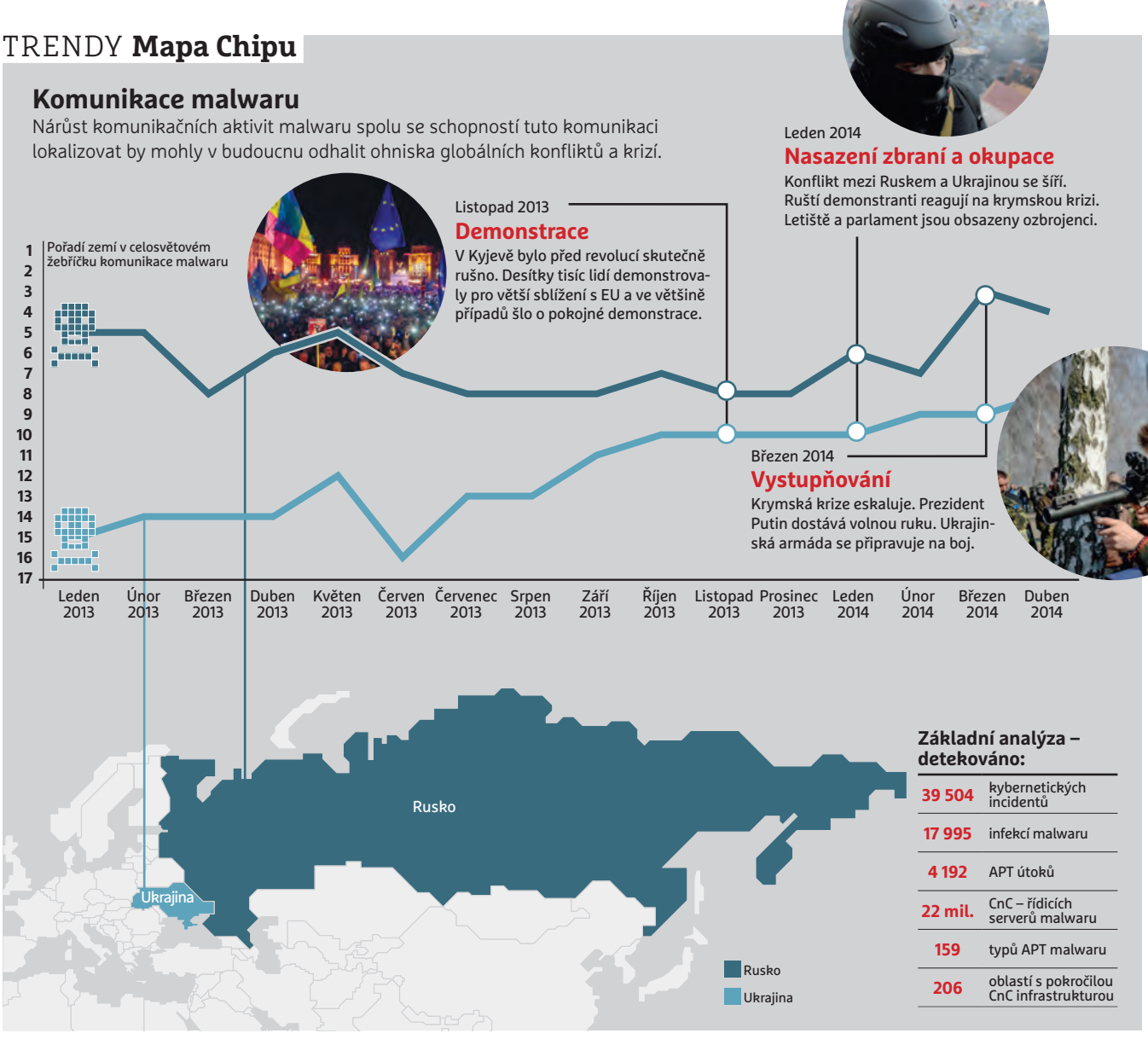

Dokáže malware předpovědět nadcházející krizi?

Těsně před vypuknutím krymské krize byl detekován zvýšený počet komunikačních spojení malwaru. Podle bezpečnostních expertů by detekce podobných událostí mohla být využita pro predikci budoucích krizí.

Podle bezpečnostních expertů ze společnosti FireEye může nyní malware sloužit i jako systém včasného varování před hrozící krizí. Studie ukazují, že s malwarem spojené hrozby nebo náznaky kybernetické války často předcházejí skutečné konflikty.

Zjištění společnosti FireEye bylo založeno na komunikačních údajích spojených s malwarem, který byl detekován na více než 5 000 počítačích firem a veřejného sektoru. Ve většině případů šlo o komunikaci mezi malwarem a jeho řídicím serverem, od kterého škodlivý kód přijímal nové příkazy, často spojené s aktualizací. Je například prokázáno, že když byla rozpoutána krymské krize, rapidně se zvýšila aktivita škodlivých programů, která vzrostla především u serverů v blízkosti Krymského poloostrova. Experti odhadují, že za tuto aktivitu malwaru jsou zodpovědné různé vládní organizace, které chtěly z této oblasti shromáždit co nejvíce informací.

Podle společnosti FireEye lze umístění hackerských aktivit poměrně snadno identifikovat, protože při takovýchto událostech jsou jen málokdy využívána opatření zakrývající jejich umístění.

Další příklad scénáře, v němž vstoupil do hry takovýto „malwarový systém včasného varování", představoval konflikt mezi Hamasem a Izraelem v pásmu Gazy. V období, kdy se Izrael připravoval k prvnímu útoku, došlo k rapidnímu nárůstu datového provozu. Vzhledem k tomu, že se zmiňovaný provoz týkal i USA a Kanady, existuje podle FireEye podezření, že v těchto dvou zemích je přítomna izraelská infrastruktura. Podle některých teorií je dokonce možné, že konflikt byl ovlivněn i tajnými službami obou zmiňovaných zemí.

V každém případě je ale jasné, že pomocí analýzy datového provozu škodlivého kódu by v souvislosti s globálními událostmi bylo možné odhalit nebezpečné politické krize – ještě předtím, než naplno vypuknou.

autor@chip.cz

FOTO: THINKSTOCK/GLEB GARANICH/KONSTANTIN CHERNICHKIN/MAKS LEVIN (V. LI. N. RE.)
ZDROJ: HTTP://WWW.FIREEYE.COM/BLOG/AUTHOR/KENNETH-GEERS