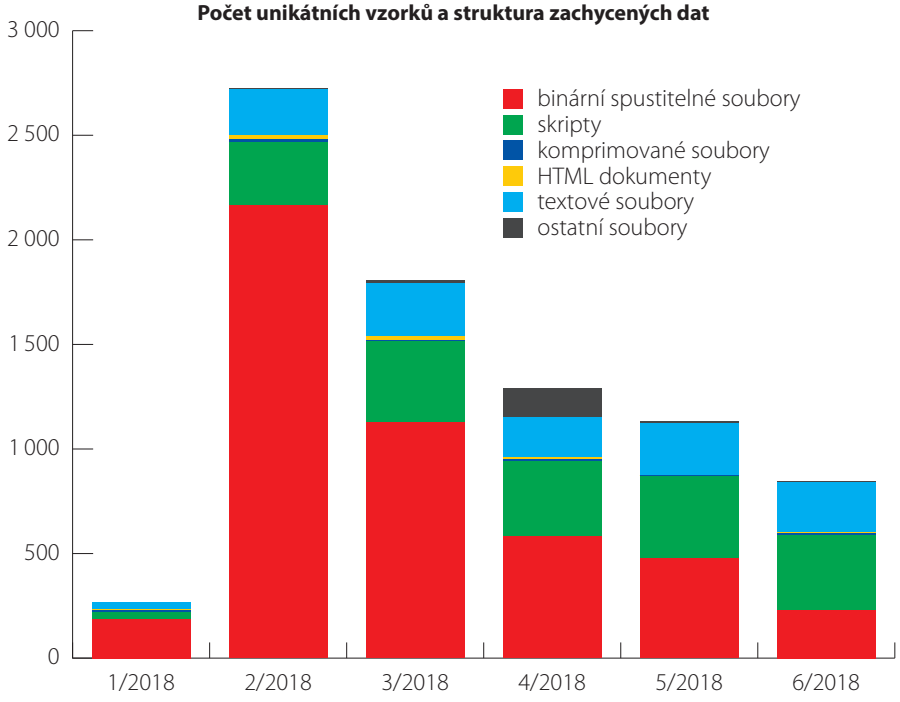
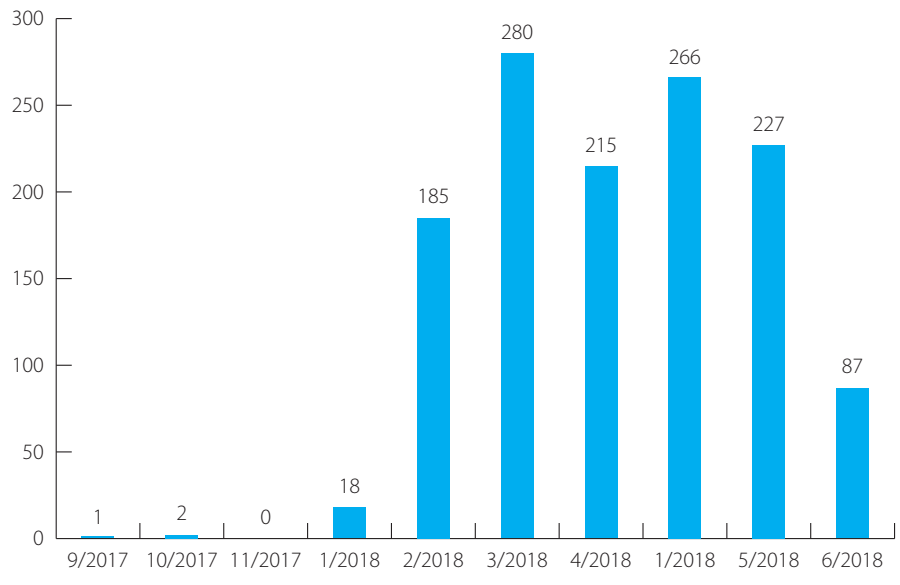
Počet unikátních vzorků a struktura zachycených dat



Průměrný počet útoků na jednoho uživatele



Taková komunikace vypadala typicky tak, že po úvodní inicializaci docházelo pouze k pravidelnému udržování spojení (keep-alive). Další zachycené vzorky se snažily připojit do takzvaného těžebního poolu, kde bylo jejich úkolem těžit virtuální měnu pro útočníky.

U jiných vzorků se zase zaznamenala snaha o DDoS útok, která se ale později projevila jako snaha o detekci schopnosti napadeného počítače podvrhovat zdrojové IP adresy.

Na rozdíl od DDoS útoku se malware pokusil poslat pouze několik paketů s odlišnou zdrojovou IP adresou na adresu svého (C&C) serveru. V případě, že by se detekovalo, že čerstvě získaný počítač toho schopný je, byl by s největší pravděpodobností zneužit právě k DDoS útokům.

Ty dnes patří k velmi častému typu útoku, jehož cílem je vyčerpání prostředků cíle, který nemá šanci poznat, zda jde o legitimní požadavek uživatele zobrazujícího obsah webových stránek, nebo uměle vygenerovaný provoz.

Analýza dat z veřejného honeypotu ukázala, že útoky na domácí routery představují bohužel každodenní realitu.

Dbát na bezpečnost svého routeru by tak mělo být stejnou samozřejmostí, jako používat antivirový program. ■

Autor pracuje ve společnosti CZ.NIC