Jelikož velké množství škodlivého softwaru používá internet, nabízí se možnost detekovat infikované počítače na základě kontroly síťové aktivity. Útočníci však skrývají obsah komunikace tím, že využívají šifrované protokoly jako je například HTTPS, takže se při analýze síťové komunikace musíme spolehnout na metadata. Společnost Cisco nám poskytla dataset obsahující agregovaná metadata doplněná o informaci, zda daný vzorek komunikace obsahoval nežádoucí aktivitu. Tato práce se zabývá tím, jak naučit neuronové sítě na základě těchto metadat detekovat nežádoucí komunikaci. Srovnává jednotlivé architektury a také porovnává výsledky neuronových sítí s výsledky jiných metod strojového učení použitých našimi kolegy. Také se pokouší vytvořit zobrazení, které zobrazuje vzorky komunikace do prostoru, kde vzorky škodlivé komunikace vytvořené jednou rodinou škodlivého softwaru vytvářejí klastry. Takové zobrazení by mohlo pomoci najít další počítače napadené virem na základě vzorku komunikace tohoto viru, a to i v případě, že tento virus není detekován detekčním systémem.