Počítačové viry a bezpečnost počítačových systémů
Protokol z předmětu (2b)

Tématická oblast: Windows API, registry, oprávnění

Přednášející: prof. Ing. Ivan Zelinka, Ph.D.; Ing. Jan Plucar, Ph.D.
Cvičící: Ing. Jan Plucar, Ph.D.

Jméno a číslo studenta: Daniel Trnka, TRN0038
Datum vypracování: 2. 3. 2019

Zadání:

1) Seznamte se s Windows API z pohledu programátora.
2) Seznamte se s Windows registry a jejich použitím přes Windows API.
3) Zjistěte, jak je možné automaticky spouštět aplikace po startu Windows (především pomocí registrů).
4) Rozšiřte Váš keylogger z minulého cvičení - keylogger při startu zjistí, zda v registrech existuje záznam, který spouští tento program:
    a. Neexistuje-li záznam, který by spustil program z aktuálního umístění, vytvořte jej.
    b. Existuje-li záznam, který spouští Vámi vytvořený program z umístění, které ovšem již neexistuje, nahraďte jej cestou k aktuálnímu souboru.
    c. Existuje-li záznam s hodnotou odkazující na existující umístění Vašeho keyloggeru, neprovádějte žádnou akci.
5) Dále rozšiřte keylogger o tuto funkci: Vyžádejte oprávnění administrátora a přes shell vypněte firewall.

Závěr:
Do tohoto protokolu nemusíte vkládat screenshoty. Společně s protokolem ovšem odevzdejte zdrojové kódy Vašeho keyloggeru. Binární verze programů neodevzdávejte.

Diskutujte následující témata:
1) Jmenujte další způsoby, jak je možné spouštět malware při/po startu systému.
2) Co je UAC? Jak funguje a k čemu slouží?
3) Diskutujte metody, jakými může malware získat administrátorská oprávnění na Windows systémech (je-li aplikace spuštěna pod běžným uživatelem).