Обнаружение таргетированной атаки на практике

Максим Лукин
Руководитель направления Информационная Безопасность
CTI

Руслан Иванов
Системный инженер-консультант
Cisco

Communications Technology Innovations

Dark Market Silk Road 3.0

Трояны и другое интересное ПО

Escrow ✈ **Monetizing a RAT**
$8 USD / 0.029695 BTC
Vendor: **etimbuk** **+2523** **verified**
Category: **Others**
Ships From: **Worldwide...** Ships To: **Worldwide**

Remote Administration Tools/Trojans

1. Cerberus 1.03.4 BETA
2. Turkojan 4 GOLD
3. Apocalypse 1.4.4
4. Spy-Net 2.6

Rar password: Spy-Net

5. Pro Rat v1.9
6. Poison Ivy 2.3.2
7. Bandook Rat v1.35
8. Bifrost v1.0
9. CyberGate v.1.01.0
10. Lost Door v4.2 LIGHT
11. Beast 2.07
12. Shark v3.0.0
13. Sub7 v2.2
14. Pain RAT v0.1
15. xHacker Pro v3.0
16. Seed v1.1
17. Optix Pro v1.33
18. Darkmoon v4.11
19. CIA v1.3
20. Y3k RAT v1.0
21. MiniMo RAT v0.7
22. NetDevil v1.0
23. Deeper RAT v1.0
24. Schwarze Sonne RAT 0.1 Public Beta 2
25. Schwarze Sonne RAT 0.7
26. Schwarze Sonne RAT 0.8
27. Schwarze_Sonne_0.5_Beta
28. Schwarze Sonne RAT 0.2 Beta
29. [BUGFIX]SS-RAT 0.4 Final
30. A32s (fifth) RAT
31. Arctic R.A.T. 0.0.1 Alpha
32. CyberGate v1.02.0
33. CyberGate v1.03.0

How I banked in $14,580 in 14 Days

Price: $.99 USD / **0.003674 BTC**

Android App Profits

Price: $.99 USD / **0.003674 BTC**

Ultra Hacker Tools with 83 RATs and 21 Binders

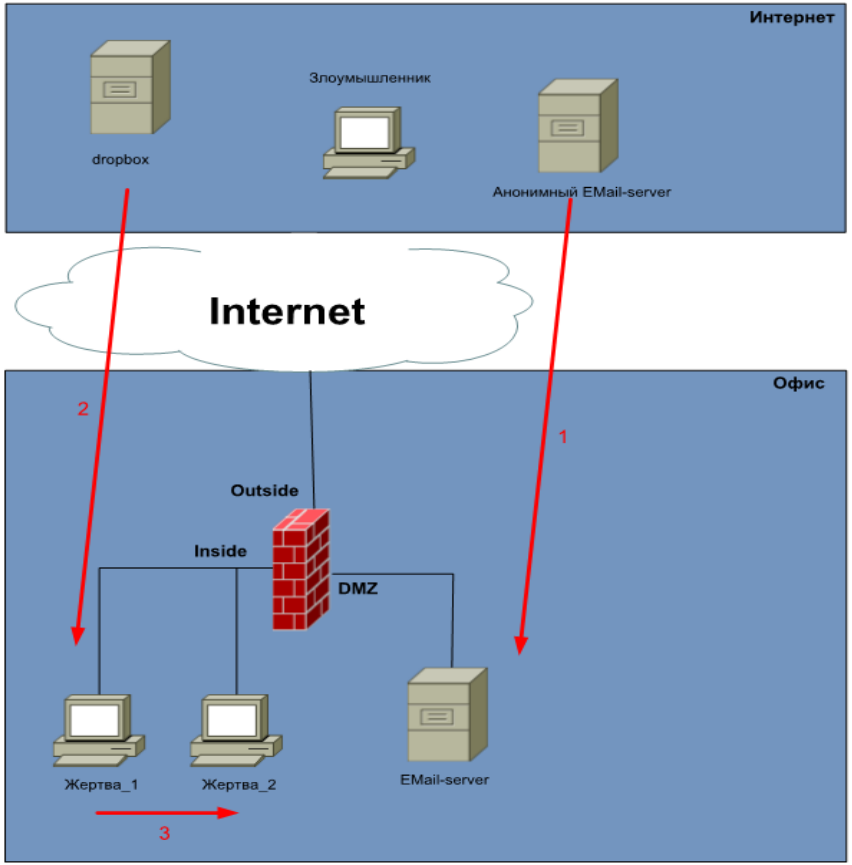
Price: $50 USD / **0.185597 BTC**

Place Order

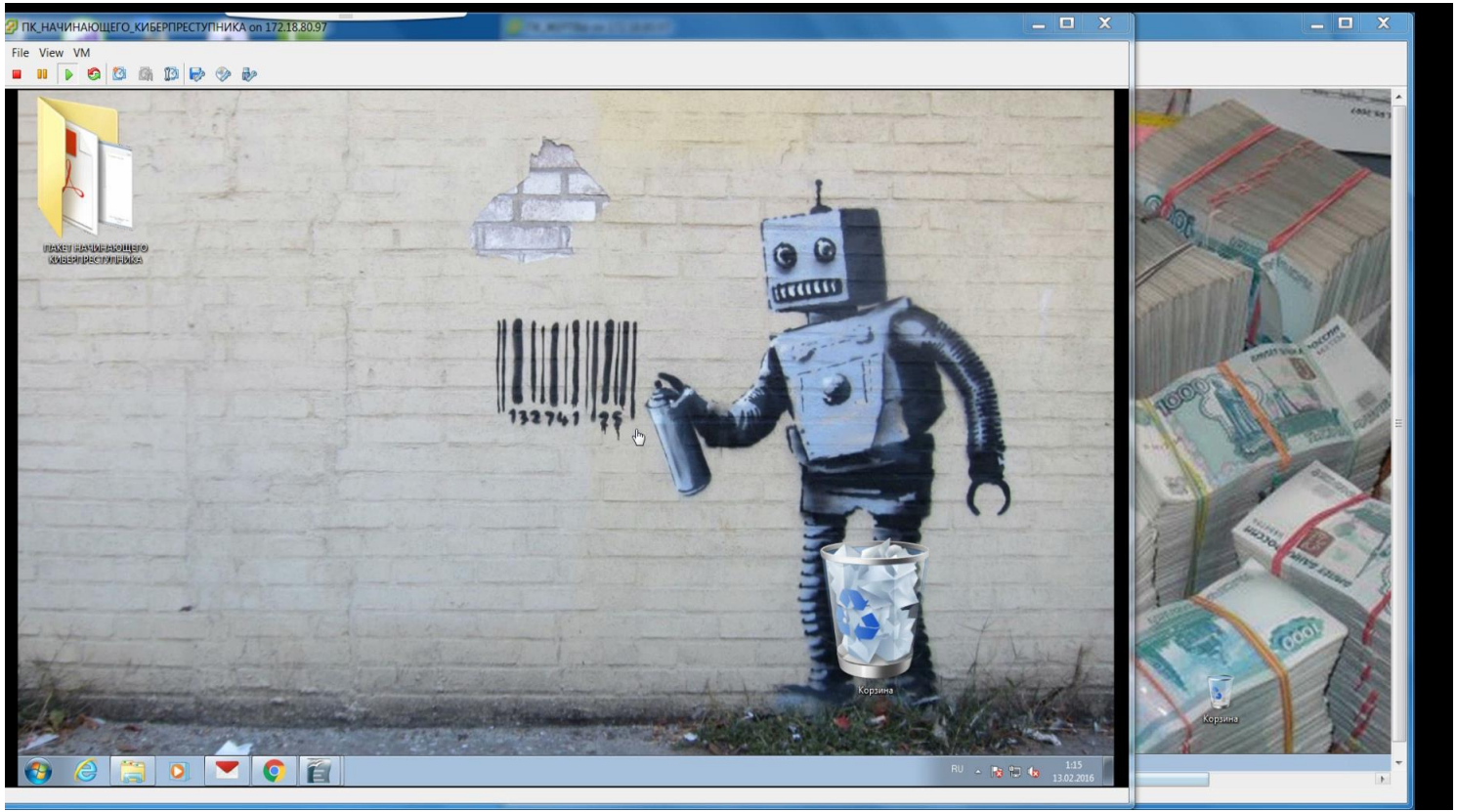
Price: $50 USD / 0.185597 BTC

Схема реализации

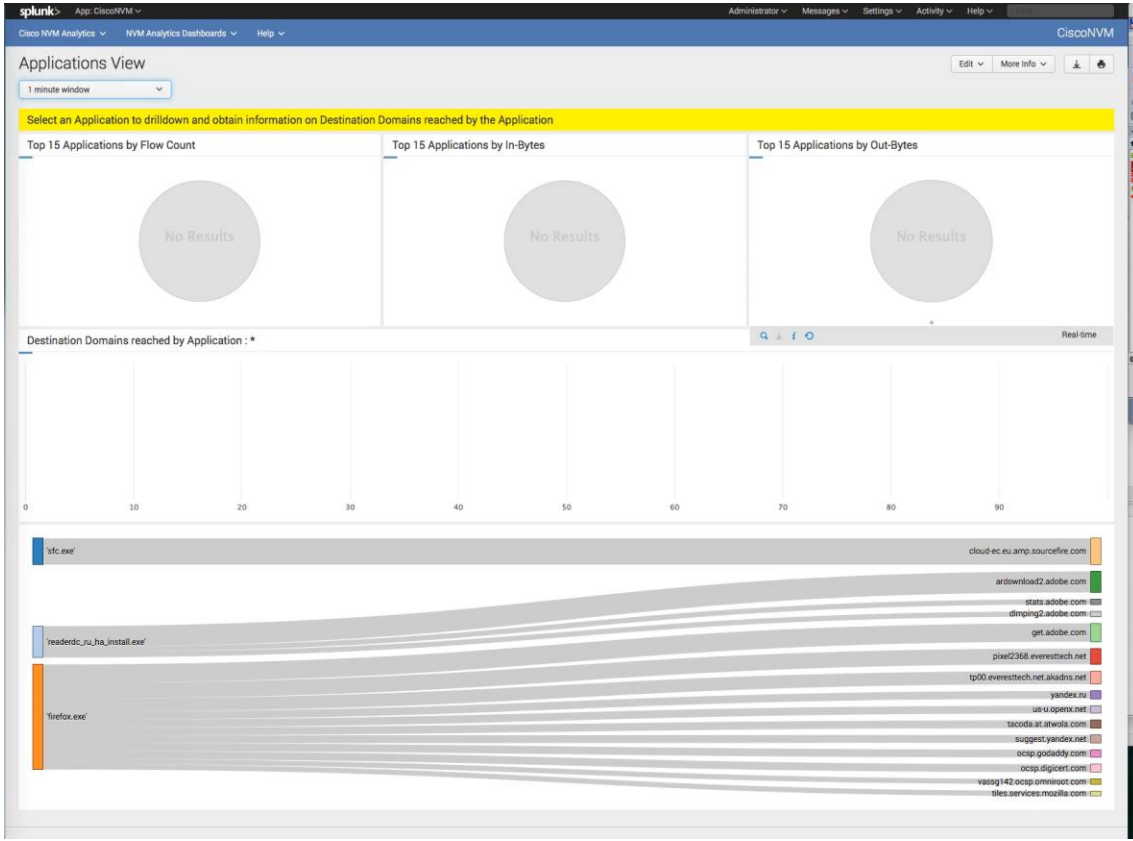
- Для демонстрации APT разработали ПО
- По направлено на кражу данных
- Rar,doc,docx,xls,xlsx,rtf,pdf,dbf,jpg,7z,tar,gzip,jpeg, psd,cdr,dwg,max,bmp,gif,png,ppt,pptx,txt,pdf,djvu,htm,html,mdb,cer,p12,pfx,kwm,pwm,1cd,md,mdf,dbf,odt,ods,accdb,ai,raw
- Локальные диски, съемные устройства и подключенные сетевые папки

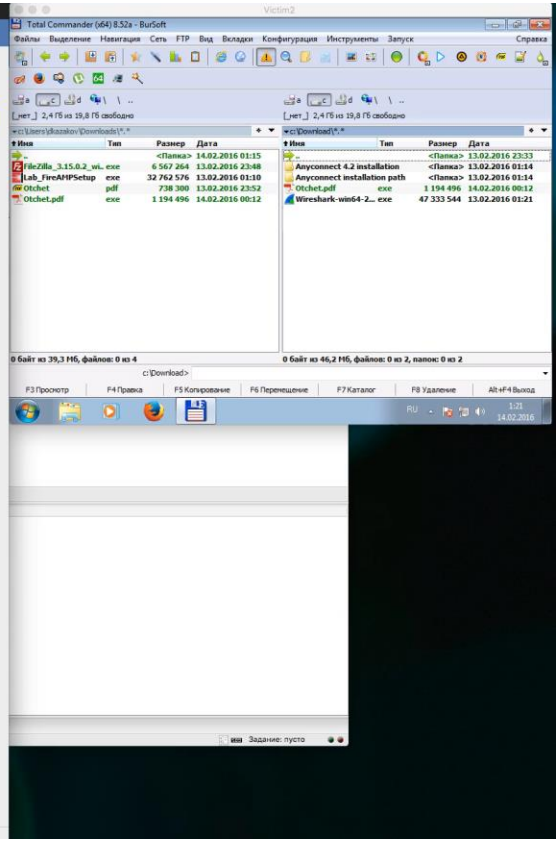


Демонстрация APT



Обнаружение APT





Заполните анкету на стенде CTI и получите доступ!

Спасибо!

Communications Technology Innovations