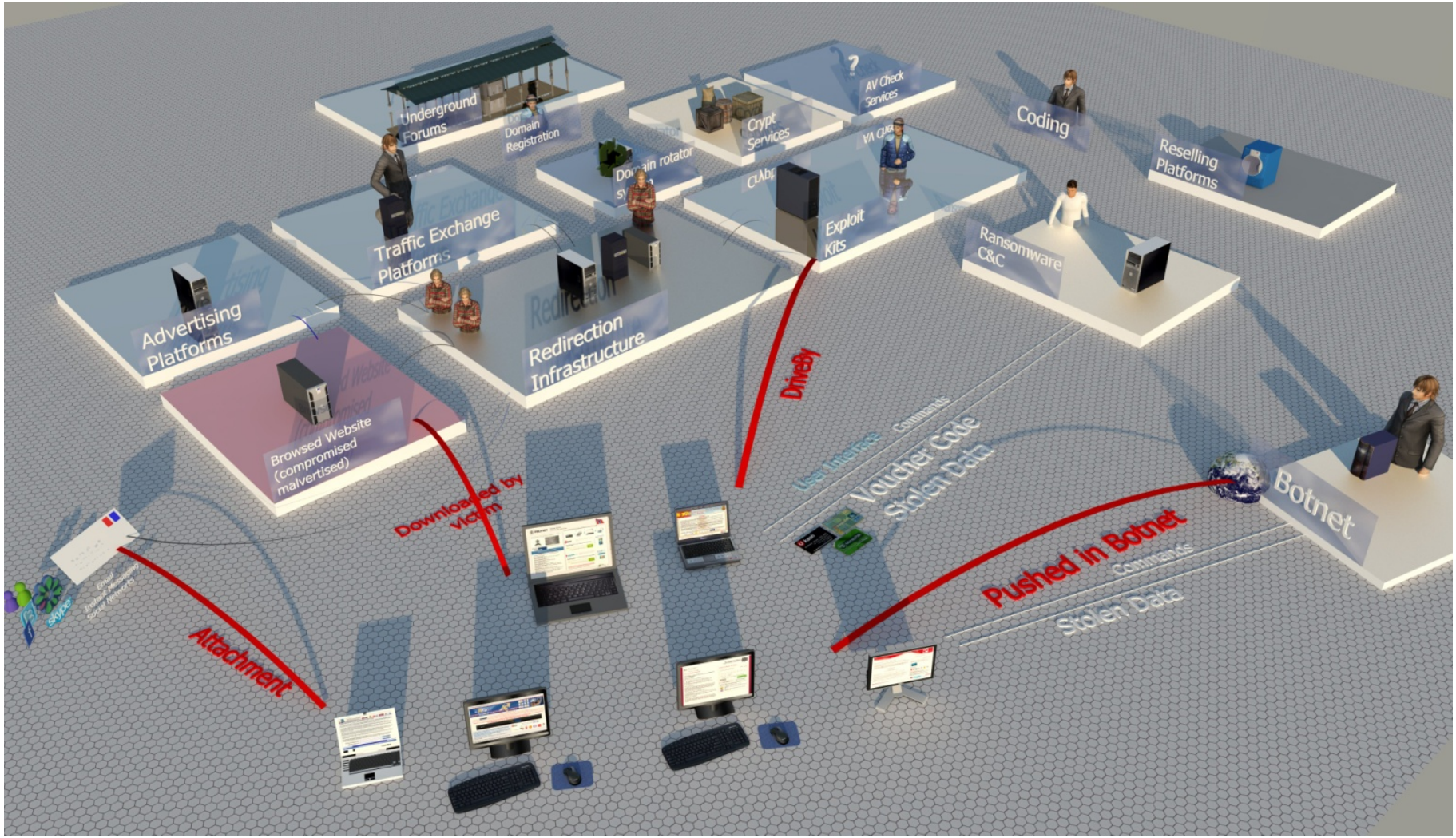
La "prima linea" delle frodi

Angelo Dell'Aera

Banche e Sicurezza 2013
Roma, 6/6/2013

L'underground russo - The Big Picture



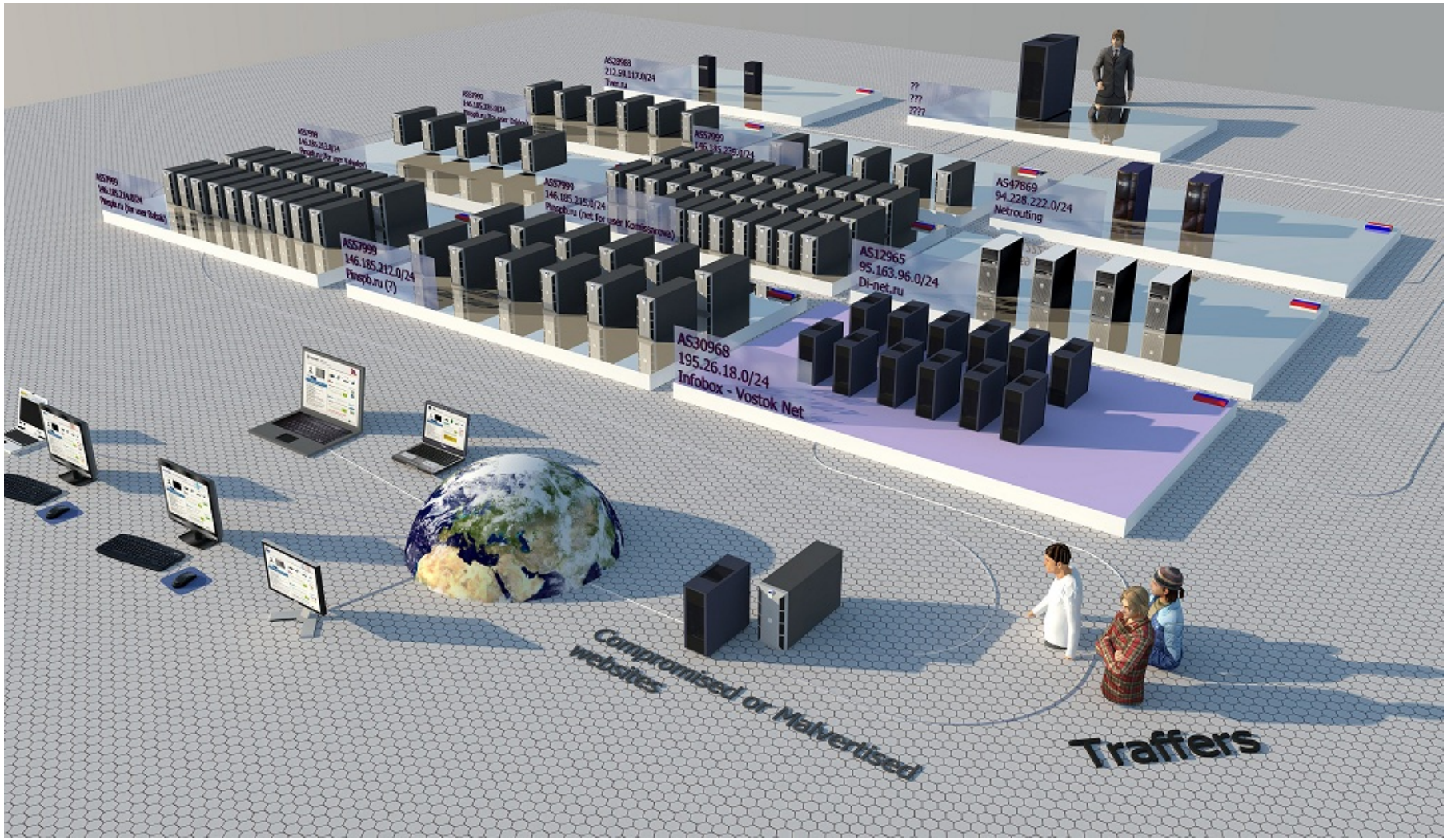
Reply
Living network

- La maggior parte degli elementi rappresentati in figura potrebbero essere teoricamente costituiti da un singolo nodo

- Nella realtà anche i gruppi criminali più piccoli e meno attrezzati sono in grado di nascondere il server che ospita realmente il contenuto malevolo dietro redirector piuttosto che reverse proxy. E' infatti estremamente più facile ricreare un redirector piuttosto che un nuovo server una volta che un nodo non dovesse essere più utilizzabile, ad esempio a causa di un blocco dovuto a blacklist di protezioni interne del browser, antivirus o altri strumenti di filtraggio

- Solitamente i gruppi più piccoli hanno a disposizione un server a cui sono associati più indirizzi IP mentre i gruppi più attrezzati hanno a disposizione un server e un redirector con IP multipli. Si tenga presente che i gruppi più attrezzati sono inoltre in grado di aggiungere ogni giorno molti redirector a questa infrastruttura aumentandone enormemente l'efficacia

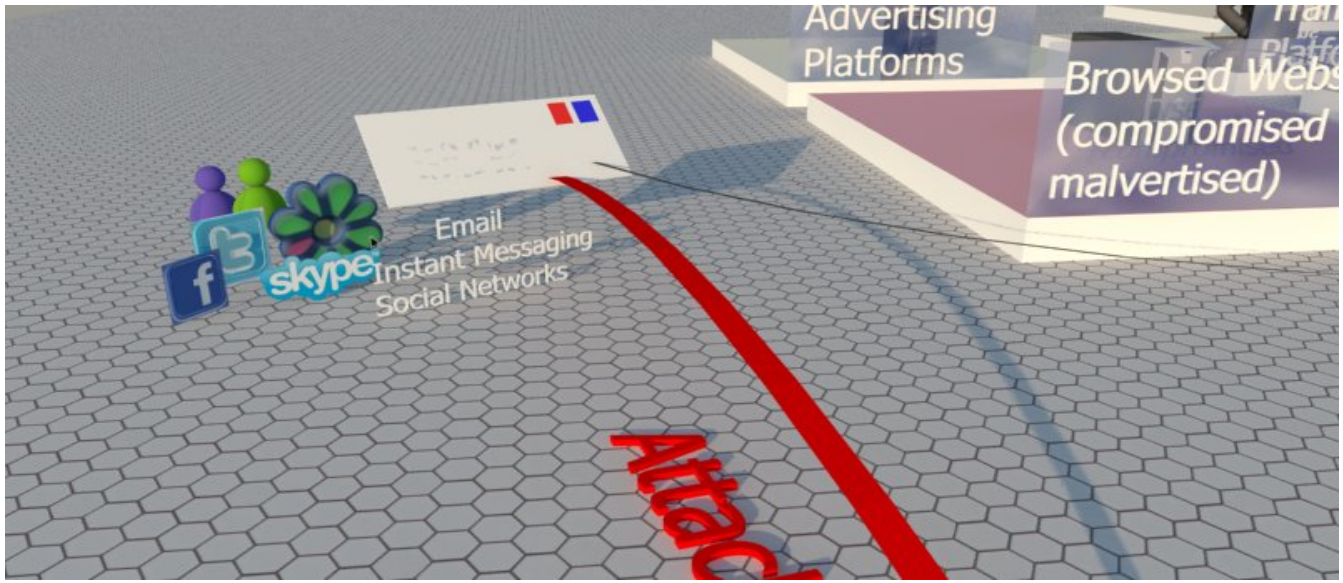
Exploit Kit - Redirezione



Reply
Living network

• Navigazione su un sito che sia stato compromesso o utilizzando una vulnerabilità (di solito relativa a un CMS non aggiornato) oppure utilizzando le credenziali rubate al legittimo proprietario

• Tale sito viene modificato per reindirizzare, ad esempio tramite l'aggiunta di un iframe, i visitatori verso l'infrastruttura di cui si parlava in precedenza



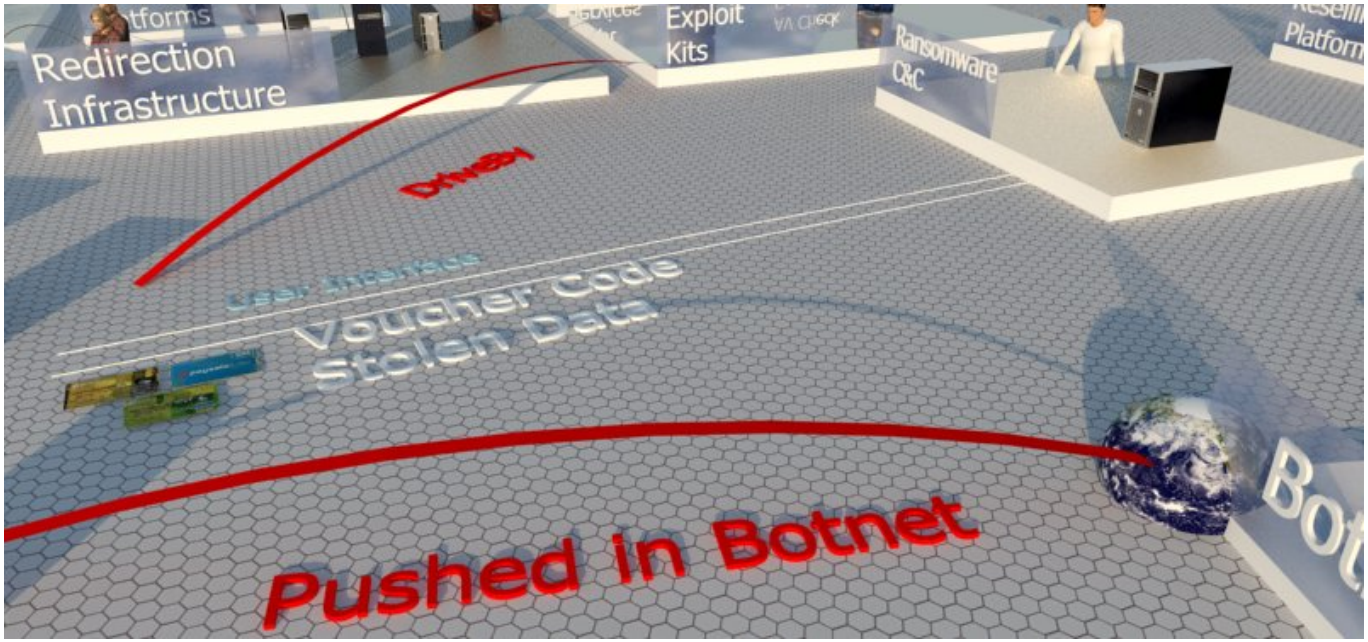
• Link che vengono “pubblicizzati” mediante chat e che conducono l’utente ignaro alla navigazione su un sito compromesso

• Email che possono contenere ancora un link a un sito compromesso oppure allegati che contengano direttamente un eseguibile piuttosto che un documento (ad esempio PDF) contenente un exploit

200	HTTP	delivery.trafficbroker.com	/rd.php?http://teen-fuck.com/	209
302	HTTP	teen-fuck.com	/	5
200	HTTP	haztalanhardad.bounceme.net	/JaOqWY?QbJdL=13	1 094
200	HTTP	haztalanhardad.bounceme.net	/kgr3r9BB9nX	17 608
200	HTTP	haztalanhardad.bounceme.net	/kgr3r9BB9nX	17 608
200	HTTP	haztalanhardad.bounceme.net	/PuqaJL?pQIO=12&sQJo=1251	137 216

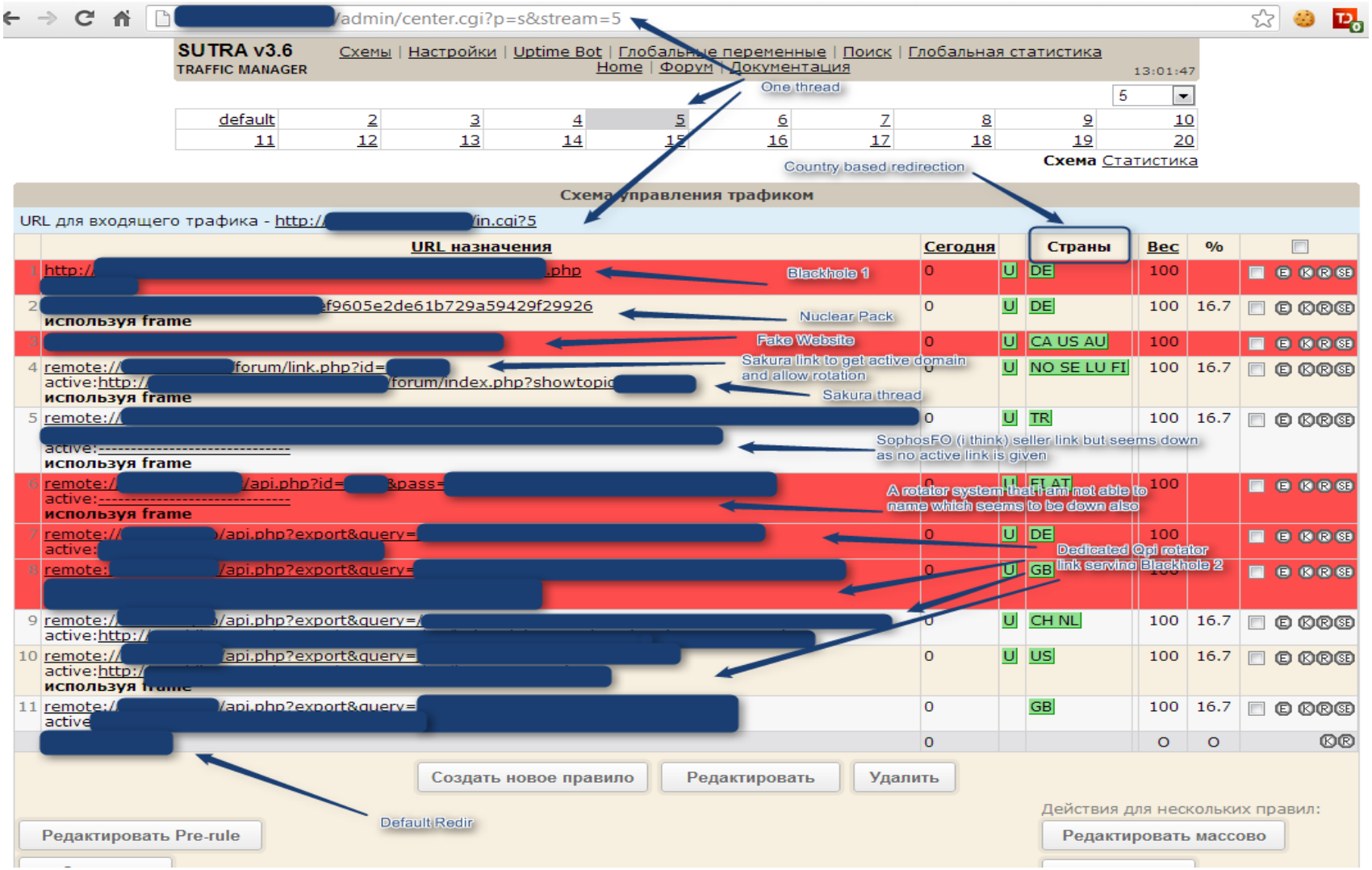
• Piattaforme di advertising (legittime oppure no)

• Tali piattaforme vengono usate (o abusate in alcuni casi) dai criminali per pubblicizzare mediante advertisement falsi siti tipicamente porno. In questo caso, l'utente innesca la catena di redirezioni cliccando sull'advertisement



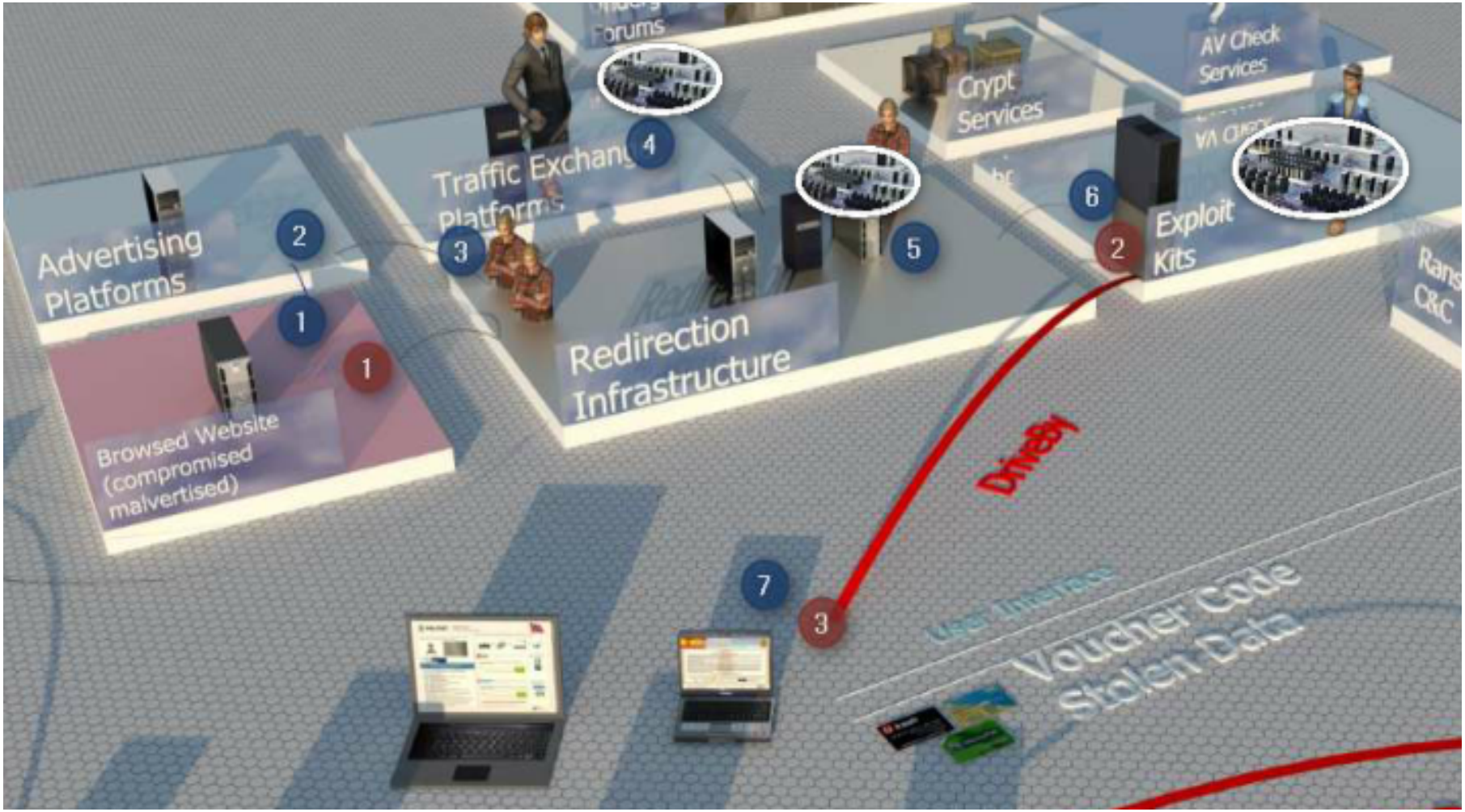
• Un malware viene installato su una macchina già infetta e appartenente a una botnet

• Non è raro infatti che su una macchina già infetta vengano iniettati altri malware differenti da quello già inizialmente presente

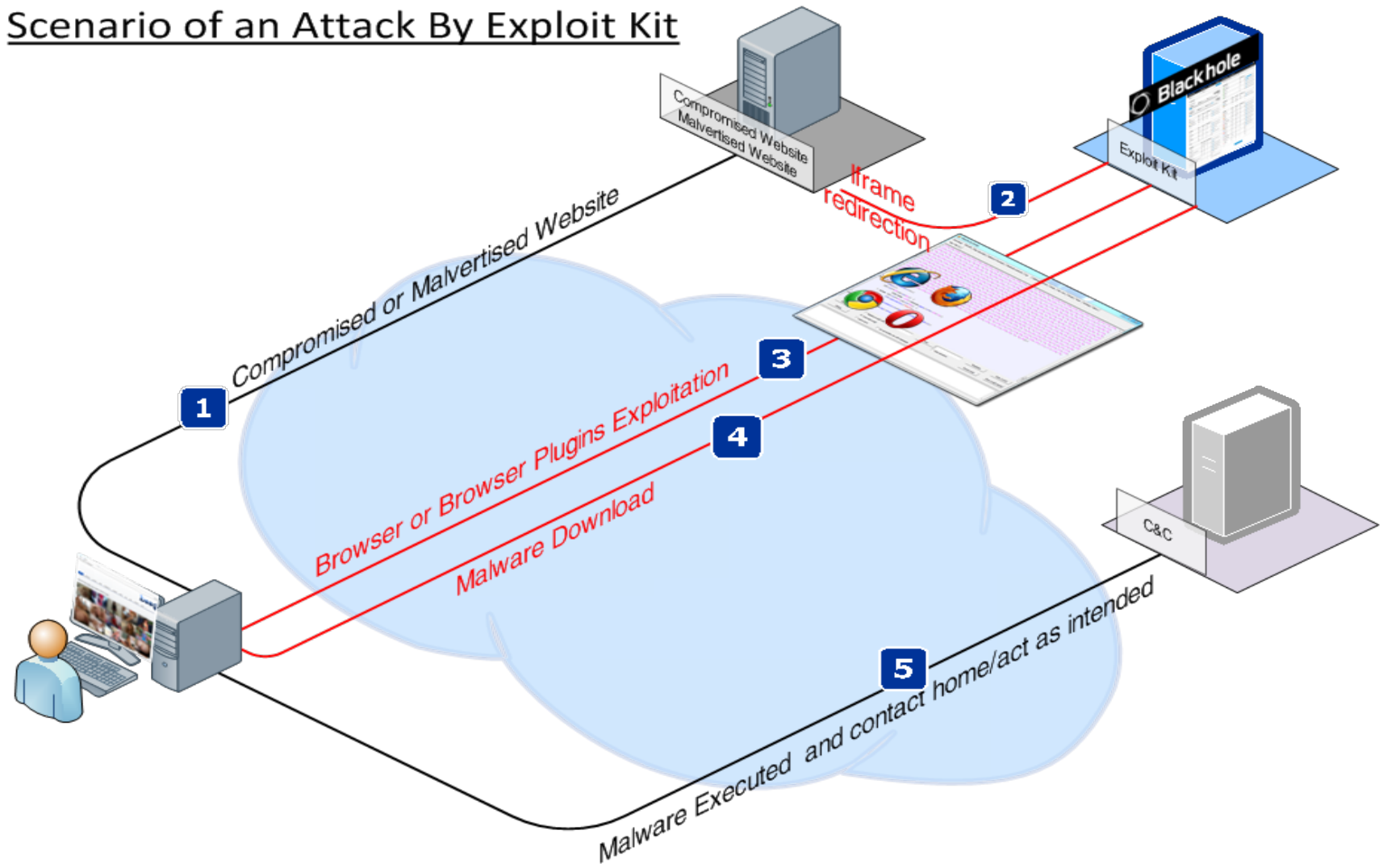


Reply
Living network

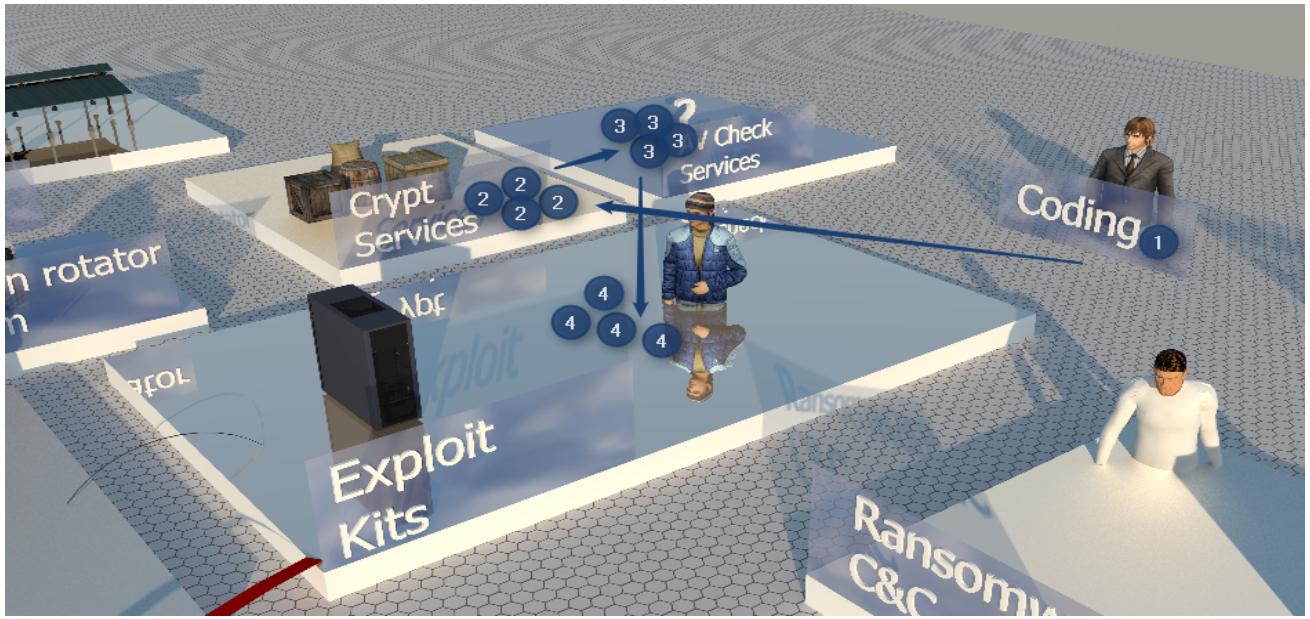
Cosa succede davvero…



Reply
Living network



Reply
Living network



• Esistono infatti numerosi servizi che consentono di effettuare repacking e cifratura di tali eseguibili in maniera molto efficace

• Lo scopo di questi servizi è quello di eludere le signature di rilevazione dei più noti software antivirus/antimalware nonché quello di modificare piccoli ed inutili dettagli dell'eseguibile al fine di modificarne l'hash

- Malware Don’t Need Coffee Blog

  “*The path to infection - Eye glance at the first line of "Russian Underground" - focused on Ransomware*”
  http://malware.dontneedcoffee.com/2012/12/eyeglanceru.html

Contatti

Angelo Dell'Aera
Senior Security Consultant
Communication Valley Reply
a.dellaera@reply.it