T : , , T T T

L , J 7 , *M b , IEEE*, , *S M b , IEEE*, ,
L L

***Abstract*— Tor is a popular low-latency anonymous communication system. It is, however, currently abused in various ways. Tor exit routers are frequently troubled by administrative and legal complaints. To gain an insight into such abuse, we designed and implemented a novel system, TorWard, for the discovery and the systematic study of malicious traffic over Tor. The system can avoid legal and administrative complaints, and allows the investigation to be performed in a sensitive environment such as a university campus. An intrusion detection system (IDS) is used to discover and classify malicious traffic. We performed comprehensive analysis and extensive real-world experiments to validate the feasibility and the effectiveness of TorWard. Our results show that around 10% Tor traffic can trigger IDS alerts. Malicious traffic includes P2P traffic, malware traffic (e.g., botnet traffic), denial-of-service attack traffic, spam, and others. Around 200 known malwares have been identified. To mitigate the abuse of Tor, we implemented a defense system, which processes IDS alerts, tears down, and blocks suspect connections. To facilitate forensic traceback of malicious traffic, we implemented a dual-tone multi-frequency signaling-based approach to correlate botnet traffic at Tor entry routers and that at exit routers. We carried out theoretical analysis and extensive real-world experiments to validate the feasibility and the effectiveness of TorWard for discovery, blocking, and traceback of malicious traffic.**

***Index Terms*— Tor, malicious traffic, intrusion detection system.**

J 18, 2015; 31, 2015 J 22, 2015; J 22, 2015. 7, 2015; S 25, 2015. T T 2013, 013503, 61502100, 61572130, S 61532013, 61502098, 61502099, 61272054, 61202449, 61402104, 61320106007, (195819339), S 1116644, S 1350145; S S 1117175, J 20150637, 20150628; S 20150629, J T & 2014603, J 2003201, L S L 93 -9. , , , . T . L J. L , S 210096, (S : 7 . . ; . .). , 8 3 6, (- ; S . .). T , T , 21252 (- : S .). , L , 01854 (- S : . .). L :// . . . 10.1109/T .2015.2465934 S 1556-6013 © 2015 :// . . / / S

T

T S T

1 . , T . T T . T (. ., 2 , S , 1) T *dd c* (&) T . T - , . , (3 3) T , T . T . T , , . , T ( ) . , 4 . T S , T - - . T T . , 2 , T - . , T . , , . , *aM* 5 2008. *aM* 6 T T 2010. , *To Wa d*, ( ) T S S , T . T 7 T T

1 . 2 2013, . S / .

29 , $\mathcal{P}(b)$

.

$16Mb/$, -

$80Mb/$. 5

$\mathcal{P}(b)$.

$\mathcal{P}(16)$ 100%

T 260 ,

$\mathcal{P}(80)$ 100% T

$80Mb/$ 45 . ,

,

.

T . = , $\mathcal{P}_{=}(b)$

100%. T , T

$$T = a\ \{E(\mathcal{T}^1), \ldots, E(\mathcal{T}), \ldots, E(\mathcal{T})\}, \quad (3)$$

$E(\mathcal{T})$

.

T . λ

.

T_1 T

(-1)

. T

$$\mathcal{T} = T_1 + \cdots + T . \quad (4)$$

T $T_1, \ldots, T$

$E(T) = 1/\lambda$.

T ,

$$E(\mathcal{T}) = /\lambda . \quad (5)$$

T T

$E(\mathcal{T})$

,

$$T = a\ \{\frac{}{\lambda_1}, \frac{}{\lambda_2}, \ldots, \frac{}{\lambda}\}. \quad (6)$$

T

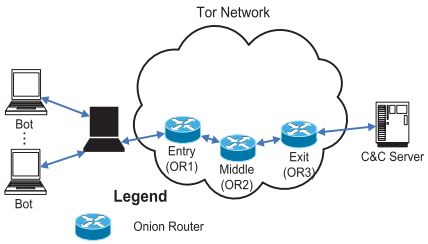
T. (6)

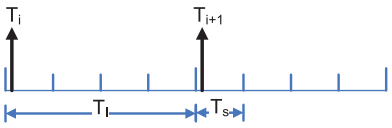
.

T

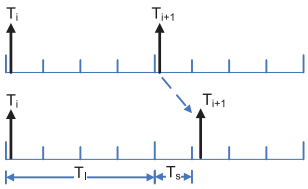
.

. S T T S T T L , L S S T L S

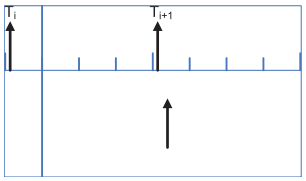

Tor Network
Bot
Bot
Entry
(OR1)
Middle
(OR2)
Exit
(OR3)
C&C Server
Legend
Onion Router



. 14. S -



. 15. S



C. I ● DTMF ● T ac bac

S T .

- .

T , ?

, .

- , .

.

?

- ? -

?

.

. L S S

, T

: ( ) ,

( ) , ( )

. ,

: .

A. I c ● N●

T ,

. 14

- . T -

T .

, .

, T -

( ) , -

. T .

T -

, :

Ca 1 (C S):

1 $\{T_1, \ldots, T\ \}$,

. T_α - 3

2, T_β - 2

1. 2 T_η. ,

T T_{+1} ,

$$T_{+1} = T\ + T_I + T_\alpha + T_\beta + T_\eta, \quad (9)$$

$1 \leq\ <$ T_I

.

T_I , F_I
, $^{2\pi F_I} = (2\pi F_I) + (2\pi F_I)$
c . ,
c d a , M c c a F_I a
- a M d . T , P
,

$$P = \sum_{=-\infty}^{\infty} |c|^2, \tag{13}$$

$|c|^2$
.
, -
,
$'( )$,

$$'( ) = ( ) + \zeta, \tag{14}$$

$( )$
. ζ Ga a
( ) , $N(0, \sigma^2)$.
,
P' $'( )$,

$$P' = \frac{1}{2\ell} \int_{-\ell}^{\ell} (( ) + \zeta)^2 \, d \, , \tag{15}$$

,

$$E(P') = E\left(\frac{1}{2\ell} \int_{-\ell}^{\ell} (( ) + \zeta)^2 \, d \right) \tag{16}$$
$$= \frac{1}{2\ell} E\left(\int_{-\ell}^{\ell}) \right)$$

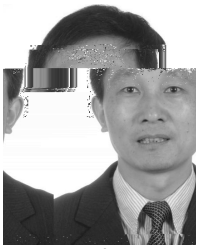
, . ., 16 18 .
,
. T
.
S
. L S
, , *T● Wa d*,
, ,
T . , *T● Wa d*
T -
S
T . ,
,
2 , , , ,
T . 3, 624, 700
, 78.03% 2 ,
8.99% . T
,
M T● Wa d, S
T . T -
, -
- (T)
T .
,
T . T *T● Wa d*
- .

1 T T , . (2015). *T● : A ● O M* . . : // . . /
2 . , T : , *P ●c. 22 d I . W● M W d W b C●* . *(WWW)*, 2013, . 213 224.
3 . , J. L , . , . , - - L , *P ●c. 32 d IEEE I . C● . C●* . *C●* . *(INFOCOM)*, . 2013, . 1043 1051.
4 . . (2011). *F d b IP: D● I Ta C a ● R a T● E S R M ?* . : :// . . /18892/
5 . , . , . , T. , . , S : T , S *P ●c. 8 I . S P ac E a c T c ●M(PETS)*, 2008, . 63 76.
6 . , . , . . , : T , *P ●c. 4 I . C● . N . S . S c . (NSS)*, 2010, . 167 174.
7 . , J. L , . , . , . , T : L T , *P ●c. 33 IEEE I . C● . C● . C●* . *(INFOCOM)*, ./ 2014, . 1402 1410.
8 . . (2010). *R M B● C● a d a d C● ●M W T●* . . : :// . . / / -18/ - 18- / . / -18- -T .
9 (2015). *T● 2 b: V A ● ● W b* . . : :// 2 . /
10 . (2012). *IA A a Ma a C●d a d B● O a ●, AMA*. . : :// . . / / / / 7 /
11 . . (2012). *S , a T● -P● d B● S a F● R dd* . . : :// . 7. / / / /2012/12/06/ - - - - - -
12 (2012). *D c. 2012 S T● B● /T ● a .Tb● Sa M* . . : :// . . /2012/12/ -2012- - - - .
13 . . (2013). *T R ● TOR-Ba d B●* . . : :// . . /2013/07/24/ - - - - - /
14 . . (2013). *C b c a M E W T● -Ba d C&C, R -3-R●● E ● d, SPDY F● G abb Ma a B●* . . : :// . . /2013/07/02/ - - - - - - -3- - - - - - - - /
15 . . , , *P ●c. IEEE S c . P ac S . (S&P)*, 2006, . 100 114.
16 . J. , : S , *P ●c. 13 ACM C● . C● . C● . S c . (CCS)*, . 2006, . 27 36.
17 . , J. , . , . , - L T , L , *P ●c. 6 I . C● . P a C● . A M*, 2011, . 509 516.
18 . , . , .- . , T T : , , , *P ●c. 34 IEEE S . S c . P ac (S&P)*, 2013, . 80 94.
19 . T , . , T. , . , , *P ●c. 32 IEEE I . C● . C● . C● . (INFOCOM)*, . 2013, . 1797 1805.
20 (2015). *F* . . : :// . /
21 . , . , . , . , . , - S , *IEEE T a . I . F● c S c*

49 (2015). *D aM M -F c S aM* . . : :// . . / / -
50 . J. . , - T , *P c. IEEE S c . P ac S . (S&P)*, 2006, . 183 195.
51 . , . , . , T. , . , S , L - , *P c. ACM W P ac E c . Soc. (WPES)*, . 2007, . 11 20.
52 . , J. , . , . , . J , - L - L T , *P c. 16 ACM CCS*, . 2009, . 578 589.
53 (2015). *PM Lab: A O PM D M , D M - , a d Acc PM a -ScaM S c* . . : :// . - . /
54 . . (2015). *IRC: I R M C a CM* . . L :// . . /
55 . . . (2015). *T Pa S c - ca* . . : :// . . / . ? = ; = ; = - .

Zhen Ling

T S , , 2005, . . , 2014. S , , 2008S 2009, , , S , , 2011 2013, S . S S , S , , S , .



Junzhou Luo ('07)

S . S S . . , , , 1982, 1992, S 2000, . S , S . S S , , , , L . , , S T S .

Kui Wu ('07)

S . S . S , , , 1990 1993, , . . , , 2002. , , , 2002, S , . - , , T , .

Wei Yu

. S T , , , 1992, . S - T , S , , 1995, . . T & , 2008. , S , T . , , - , . S 2014.

S

Xinwen Fu

J S , , 1995, . S T , 1998, S . . T & , , 2005. S , S , L . , , , , , , T . S .