Adversary-aware IP Address Randomization for Proactive Agility against Sophisticated Attackers

Jafar Haadi Jafarian, Ehab Al-Shaer, Qi Duan

CyberDNA Center, Department of Software and Information Systems

University of North Carolina at Charlotte

Charlotte, NC, USA

{jjafaria, ealshaer, qduan}@ucc.edu

Network reconnaissance of IP addresses and ports is prerequisite to many host and network attacks. Meanwhile, static configurations of networks and hosts, especially staticness of their IP/MAC addresses, simplify this adversarial reconnaissance. Randomization of IP addresses has been suggested as a countermeasure; however, existing approaches only focus on uniformly randomizing network addresses. This fails to unleash the full potentials of this paradigm which can be realized via characterization of adversarial behavior based on network feedback to adapt the dynamics of the network to attackers' actions. In this paper, we present a novel proactive-adaptive defense technique that turns end-hosts into untraceable moving targets, and establishes dynamics into static systems by monitoring the adversarial behavior and reconfiguring the addresses of network hosts adaptively. This adaptability is achieved by discovering hazardous network ranges and addresses and evacuating network hosts from them quickly. Our approach maximizes adaptability by (1) using fast and accurate hypothesis testing for characterization of adversarial behavior, and (2) achieving a very fast IP randomization (update) rate through separating randomization from end-hosts and managing it via network appliances. The architecture and protocols of our approach can be transparently deployed on legacy networks, as well as software-defined networks. Our extensive analysis and evaluation show that by adaptive distortion of adversarial reconnaissance, our approach slows down the attack and increases its detectability, thus significantly raising the bar against stealthy scanning, major classes of evasive scanning and worm propagation, as well as targeted (hacking) attacks.

#$%&’( ) "*+,+( ) (-+ , - ." / %,’0

!"#"$%&#’ (&)*+($%"#,-+&,+.#/$0*&01&%2,+*&323"+43&#&15’ (#4+’"#-&(+3$6’&/5-’+*#,$-$"27
8+%0’ ’#$33#’%+&$3&3$4)-+7
9/#3$0’&$3&3$4)-+&/$#&%#*+15-&3+-+%"$0’&01&#""#%:&)#*#4+"+*37
;<&#((*+33&#--0%#"$0’&$3&403"-2&3"#"$%!
!+/+*#-&#))*0#%.+3&10*&;<&.0))$’6&=+*+&)*0)03+(&,5"&".+2&-#%:&+11+%"$/+’+33!
>#3+(&0’&?@A<&0*&BCD&E?2BCDF&BC!8GH&"00&$’1*+I5+’"&#’(&"*#%+#,-+7
J’$10*4&45"#"$0’&-4"3&".+&+11+%"$/+’+33&(5+&"0&-#%:&01&#(#)"$/+’+337
D.+&**60#-** 01&#(#)"$/+&45"#"$0’&$3&"0**&$’%*+#3+&,+’+1$"F&=.$-+&*+(5%$’6&%03"**7
DO&,+&#(#)"$/+F&=+&453"&**%.#*#%"+*$K+&#(/+*3#*$#-&3%#’’$’6**7"

122$%,34

!"#$%&’%()’*’%$+,-+’""%$&&+%’."/012’31/.+4/%+5%/’631#$+’71813(+’7’1.&3+&/591&316’3$"+’33’6:$%&8)5999)5:;<=<>>8)>$?)@ABCD

C--0%#"+&’+=&;<3&1*04&#((*+33&*#’6+3&".#"&.#/+&-0=+*&*$3:7
L,3+*/+&".+&3+I5+’%+&01&)*0,+3&6+’+*#"+(&,2&’+"=0*:&.03"37
J3+&3"#"$3"$%#-&.2)0".+3$3&"+3"$’6&"0&+3"$4#"+&".+$*&($3"*$,5"$0’7
D=0&.2)0".+3+3
B0’M5’$10*4$"2H&"+3"3&$1&3%#’3&#*+&3:+=+(&"0=#*(&%+*"#$’&*#’6+37
B0’M*+)+"$"$0’H&"+3"3&$1&3%#’3&#*+&#/0$($’6&*+)+#"+(&)*0,$’67
A.#’6$’6&*+#-&;<&E*;<G&#((*+33&01&.03"3&($3*5)"3&#%"$/+&3+33$0’37
;’3"+#(F&=+&#330%$#"+&.03"3&=$".&+).+4+*#-&;<&#((*+33+3&E+;<G7
A.03+’&1*04&5’53+(&#((*+33&3)#%+7
C5"04#"$%#--2&"*#’3-#"+(&"0N1*04&*;<3#"&’+"=0*:&+(6+37
B+=&+;<$3&#’’05’%+(&"0&%-$+’"3&".*056.&?B!&=$".&3.0*"&DD07
;<&#((*+33+3&#*+&45"#"+(&=$".05"&P+0)#*($K$’6&%2,+*&0)+*#"$0’&0*&,*+#:$’6&#%"$/+&3+33$0’37

5(06’+0

Non-uniformity test

!"#1("03,-0"’%3,’’8"3%-3(-+$,+(."-"02(3=D=3"$,->(0@
! E-3$(,0(0"0633(00"$,+(",-."(3$(,0(0".(+(3+,&=’=+8
! (!>!"’%3,’92$(D($(-3(B".=7=.(9,-.93%-C6($"0(C6(-+=,’
K0(":+’*%.(;%$!2%<=’*+)$&+%&$+%"3,’36’,+(")+,-’&-.($>*.1$(.*1’?$
! #97,’6("L"M!MN
ED".(7=,+=%-"=0"7($8"4=>4B"03,-0",$("-%-96-=D%$)
!/#=D",33(2+(.B":4=34"$,->(0",$(")%$("4,F,$.%60@
! O=-."$,->(0":=+4",&-%$),’"-6)&($"%D"03,-0"I%6+’=($0J
! /=7("’%:($":(=>4+0"+%"+4(0("4,F,$.%60"$,->(0

Non-repetition test

!"#1("03,--($0",7%=.=->?’=)=+=->"$(2(,+(."03,--=->@
! 5(.63(0".(+(3+,&=’=+8",-."03,--=->"&6.>(+
! (!>!"A%%2($,+=7(B".=7=.(9,-.93%-C6($
A,’36’,+("%&’()’*)$)+,-’&-.($%D"03,-".=0+$=&6+=%-
! ED".(7=,+=%-"=0"7($8"’%:B"$(2(+=+=%-"=0"’=)=+(."
!/#=D",33(2+(.B":4=34",..$(00(0",$(")%$("4,F,$.%60@
! 1..$(00(0":=+4’"%:"-6)&($"%D"03,-0
! /=7("’%:($":(=>4+"+%"+4(0("4,F,$.%60",..(00(0

0’1+234’(5-(5

! 1++,3G($H0"6.*%&$%&*’&+57$I6-=D%$)"03,--=->J"=-"%&’&-3-(+:%$G0"
&(3%)(0"4($"8+%&$%&*’&+57$-"%6$"’’)’9&-,+-(+:%$G!

! "##$%&’()**!"#"$%&’()** *+)$,$-#./’)01#$#.*23 $##$%&).4)
,(*(&&())

! 5+)$##$%&’()**#"$%&’()** *+)$,$-#./’)01#$#.*2) " +*(%’,)#*),*)
!"#$%&’ 4%$22.26)" $##$%&)7’%*0’4)**’%&(+)(*(,*-./(**