L-006

分散型走査グループの検知と攻撃ペイロードの分類

Detection of Distributed Scan Group and Classification of Attack Payloads

梶川　慶太 †　　中村 康弘 †

Keita Kajikawa　　Yasuhiro Nakamura

1. はじめに

複数の異なる IP アドレスを持つ機器のグループが協調して DoS を行うネットワーク攻撃は DDoS(Distributed Denial of Service) 攻撃として知られている．同様に，機器が接続されている IP アドレス，接続可能なポート番号，そのポートで稼働しているサービスプログラムのバージョン番号や関連する脆弱性などを調べる走査（スキャン）活動についても，複数の機器を協調して動作させる分散型走査攻撃 (Distributed Scan Attack) が考えられる．この研究では，ペイロードに基づいて，分散型走査グループの検知を行うとともに特定ポートへの接続目的の分析を行う．

2. ネットワーク走査活動

2.1. ネットワーク走査活動の分類

ネットワーク走査活動は，一般に (1) 調査：機器が存在し接続可能な IP アドレスやポート番号，サービスプログラムのバージョンなどを調べる，(2) 検証：それらが見つかった場合，そのサービスが利用可能かどうかテストする，(3) 攻撃：走査と同時に脆弱性を利用する攻撃コードを送付して意図したプログラムを実行させる，の 3 種類の意図に区別して考えることができる（図 1）．

2.2. 分散型走査活動グループの検知

分散型走査活動グループを検知するためのいくつかの既存手法が提案されている．文献 [1] では，複数の実サーバを用意して，そこへ到達する分散型走査活動パケットの特徴を抽出し，それを用いて分散型走査活動を検出する手法を提案している．また，文献 [2] ではダークネット観測結果を機械学習することで分散型走査活動検出を行っている．

この研究では，図 1(2) を前提に，TCP の接続要求に対して擬似応答を返すことで初期ペイロードを取得し，そのハッシュ値の同一性から複数アドレスのグループ化を行う．とくに本稿では得られたグループのうちのひとつに着目し，その活動履歴から，当該グループの活動特性を明らかにする．

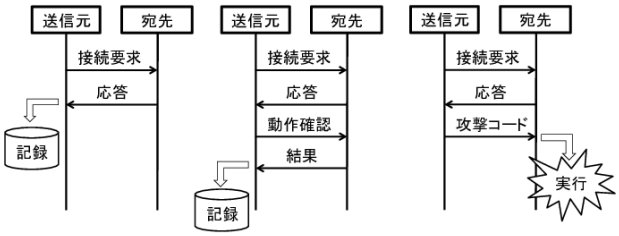
2.3. 特定ポートへの攻撃パケットの分類

2.2 で得られたグループの宛先ポートの中から特定のポート番号に着目し，そこへ送付される初期ペイロードの内容を抽出・分類して攻撃コードと意図の推定を行う．

3. 観測データの分析結果

3.1. ペイロードに基づくグループの検出

2014/1/1 から 2014/12/31 の間，観測中の約 1,500 個のアドレス範囲に対して，同日中に同一のペイロードを送付してきた複数のアドレスグループを抽出した結果，2,256 個のグループを得ることができた（同一メンバで構成されていても活動日が異なる場合は別グループとしている）．この中でとくにアドレス範囲が限定的で，かつ同一のメンバにより複数日に渡って活動していた特徴的なグループ（以下，グループ A）に着目し，その出現状況について調査した．



(1) 調査　　(2) 検証　　(3) 攻撃

図 1: 走査活動のタイプ

表 1: グループ A のアドレス範囲と接続回数

IP アドレス	アドレス数	接続回数
xx.xxx.xxx.6～253	120	165
yy.yyy.yyy.220～223	4	535
zz.zzz.zzz.110～119	10	1343
合計	134	2043

グループ A は 134 個の IP アドレスから構成され，3 つのアドレス範囲からなる（表 1）．このグループの活動時期の概要を図 2 および表 3 に示す．図 2 の横軸は日付，縦軸はグループ A の全 IP アドレスの連番，各色は宛先ポート番号である．とくに 121 番から 134 番のアドレス（第 2, 第 3 グループ）からの着信が多い．また，グループ A の接続先のアドレスは全観測範囲の一部の 2 個セグメント（512 アドレス）の範囲に限定されており，そのアドレス内で宛先が分散するように走査が行なわれていた（図 2(b)）．2014 年の全日に渡って調査したが，パケットが送付されたのは表 3 に示す日のみであり，全メンバが同一日に同一のポート番号宛てに，同一のペイロードを一斉に送付しているため，協調して動作しているものと考えられる．

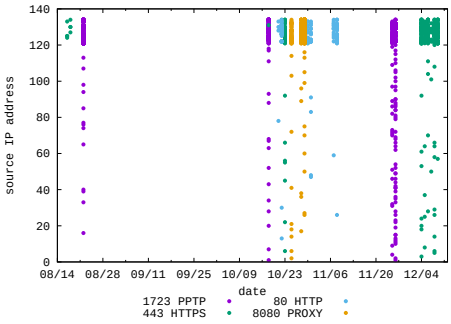
3.2.1723 番ポートに着信したペイロードの分類

3.1 で検出された表 3 の日に着信し，パケットの宛先ポート番号別にそのペイロードを分析した．とくにグループ A の宛先ポート番号のひとつ，1723 番ポート (PPTP) 宛てのパケットについて，初期ペイロードのハッシュ値を求め，同一ハッシュ値の個数を求めた後，ペイロードの内容を個別に調査した結果を表 2 に示す．宛先ポート番号が同一であっても異なる複数の攻撃意図に基づくペイロードが送付されており，

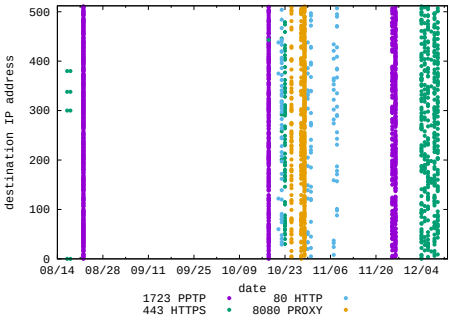
†防衛大学校 理工学研究科 サイバーセキュリティ工学

表 2: 1723 番ポートへ着信したペイロード

ハッシュ値	回数	プロトコル	内容	出処
8f623233a368d64a6b923c5eddee093d	1,474	PPTP	(null) (null)	?
318f1870e904077af7a9027f98af9eea	6,824	PPTP	(null) (null)	?
cd202ca21f679bc50c75bbaeb2ddd6a9	3,850	PPTP	"local" "cananian"	pptp-1.9.0
33e7ecd6e4962c194b6fa1bb0ababb19	1,915	PPTP	"none" "nmap"	nmap:pptp-version.nse
...(various)...	2,883	HTTP	GET / HTTP/1.0	?
4ae1711dfcecce5d75c8803540b501f8	4	HTTP	GET /nice...	nmap:TCP FourOhFourRequest
8997d4a991ea8faa3bbdf5a5705fadc0	4	HTTP	OPTIONS sip:nm SIP/2.0	nmap:TCP SIPOptions
e3173170378f294fecea500ee36f978c	4	HTTP	OPTIONS / RTSP/1.0	?
735cfdb0fdf65297e870874fd639144c	3	HTTP	OPTIONS / HTTP/1.0	?
3802e1d5ca84b70769bf49aaa7737f7e	755	Proxy	http://www.taobao.com/	?
abc55ad1d89d5f1dbebe57bd10cbc3af	5	NCP	exploit code	CVE-2012-0432
ed2b208b7ceb17b2778f6620ad7d882f	5	MMS	NSPlayer/9.0.0.2980	nmap:TCP WMSRequest
0a8ead81bef975756c87a48a83a26d6c	5	SMB	MS LANMAN	nmap:TCP SMBProgNeg
bf5301d9f66675521c734c08b9796cff	4	TNS	(binary)	nmap:TCP oracle-tns
43ee0b9006759bf99ec0702225076b93	4	SSL	(binary)	nmap:TCP SSLSessionReq
e301a56207bdbcfce3504345d52c2037	3	Kerberos	(binary)	nmap:TCP Kerberos
c99ca9a47c117c8e614795a28635b354	3	DNS	"version" "bind"	nmap:UDP DNSVersionBindReq
70078dd9273e253ea0a19ae71a72ffbe	3	-	"TNMP" "TNME"	landesk-rc
ba565feae2e281f9327855308e668a57	3	LPD	"default"	nmap:TCP LPDString
...(various)...	52	-	(binary)	?



(a) 送信元アドレスの出現日と宛先ポート番号



(b) 宛先アドレスの出現日と宛先ポート番号

図 2: グループの活動時期

また，少数ではあるが意図が不明なバイナリデータの送付も確認できた．

4. まとめ

検証の結果，類似の活動を同時に行う分散型走査活動グループの実態が明らかとなった．これらのグループのアドレス範囲については継続的に監視するとともに，その挙動や送付されるペイロードに注意する必要がある．また，1723 番ポートへ送付されたペイロードを分類した結果，必ずしも PPTP の通信を企図したものではなく，様々なプロトコルを用いた走査が行なわれていることが明らかとなった．ペイロードを調査することにより具体的な攻撃意図が明らかになるとともに，新しい攻撃ペイロードの発見にもつながるものと考えられる．今後，グループ検出の精度を高めること，および他のポート宛てのペイロードの分類を行うとともに，ペイロードの自動分類についても検討したい．

表 3: グループ A の活動履歴

年月日	送信元アドレス数	接続先ポート番号
2014/08/17	4	443
2014/08/18	4	443
2014/08/22	424	1723
2014/10/18	271	1723
2014/10/21	4	80
2014/10/22	50	80,443
2014/10/23	59	443
2014/10/25	72	8080
2014/10/28	99	8080
2014/10/29	243	8080
2014/10/30	18	80
2014/10/31	29	80
2014/11/07	16	80
2014/11/08	24	80
2014/11/25	112	1723
2014/11/26	230	1723
2014/12/04	82	443
2014/12/05	51	443
2014/12/06	69	443
2014/12/07	10	443
2014/12/08	95	443
2014/12/09	77	443
合計	2043	

参考文献

[1] Elias Bou-Harb, Mourad Debbabi, Chadi Assi, “On Detecting and Clustering Distributed Cyber Scanning”, Wireless Communications and Mobile Computing Conference (IWCMC), 1-5 July 2013.

[2] 王 サン , フォン ヤオカイ , 川本 淳平 , 堀 良彰 , 櫻井 幸一, “挙動に基づくポートスキャン検知の自動化に向けた学習アルゴリズムの提案とその性能評価”, 情報処理学会論文誌, Vol.56, No.9, pp.1770-1781, 2015.