大分大学宛ダークネット通信の解析による ゼロデイ攻撃の把握に関する一考察

東條貴明* 池部実* 吉田和幸**
(大分大学 *工学部知能情報システム工学科 **学術情報拠点情報基盤センター)

1 はじめに

インターネットにおいて脆弱性が周知・解消される前に攻撃が行われるゼロデイ攻撃が問題になっている. しかし, ゼロデイ攻撃は脆弱性に関する情報が提供される前に攻撃が行われるため IDS やファイアウォールによる対策は難しいとされている. そこで, 不正な活動に起因する通信が多く観測されるダークネットに着目する. 本研究では, 大分大学宛のダークネット通信における, ゼロデイ攻撃の予兆となる活動や送信元の特徴を調査し, ダークネットを観測することでゼロデイ攻撃の検知・把握が可能となるかを考察する.

2 ゼロデイ攻撃

ゼロデイ攻撃とはソフトウェアの脆弱性を対象とした攻撃のうち, 脆弱性の情報や対策が周知される前の攻撃行為である. 脆弱性に関する情報が提供される前に攻撃が行われるため, IDS のシグネチャによる検知やファイアウォールによる IP アドレス・ポート番号による対策が困難である.

3 ダークネット観測によるゼロデイ攻撃の把握

3. 1 ゼロデイ攻撃の調査

ゼロデイ攻撃を把握するにあたり, まずこれまでに脆弱性情報が公表された日時の前後において, ダークネット宛のトラフィックを分析してパケット数や送信元ホスト数の急激な変化などの特徴を調査する. 過去のゼロデイ攻撃の動向がダークネット上で観測できれば, その傾向を分析することで将来のゼロデイ攻撃の早期把握の参考にできる. 今回の調査は, 大分大学のダークネット上で 2015 年 11 月 1 日から 11 月 30 日までの 30 日間, pcap 形式で集計したデータを対象とした. また, 過去の脆弱性情報は脆弱性情報データベースのひとつである CVE[1]を参照した.

3. 2 観測事例

本調査において発見できたゼロデイ攻撃は 2 件あった. 1 件目は国内メーカ製の産業制御システムを標的として, 脆弱性を攻撃するツールの公開をきっかけに, 当該システムが通信に用いるポート 9600/TCP へのパケット数が急増していた.

2 件目は, X11 サーバソフトウェアを標的としたもので, ポート 6000/TCP からコマンドインジェクションを受ける可能性のある脆弱性を狙った攻撃であった. これらのうち, 2 件目の事例を詳しく述べる. 2015 年 11 月 2 日に上述の脆弱性が公表されたのに伴い, 大分大学のダークネット上でもポート 6000/TCP へのパケットの急増を観測した. 図 1 にダークネット上で観測したポート 6000/TCP 宛のパケット数を示す. 通常時の当該ポート宛パケット数は一日当たり 3000 前後で推移していたが, 脆弱性の公表された 4 日後の 11 月 6 日には通常時の 10 倍近い数の 34,827 パケットを観測した. 詳しく調査すると, ある 1 台の送信元ホスト A がパケット数の大半を占めていた(表 1). ホスト A は AbuseIPDB[2]をはじめとする IP アドレスのブラックリストに登録されており大分大学のダークネット上で不定期にパケットを観測している. ホスト C, D, E は Shodan が保有する IP アドレスであり当サービスからのポート6000/TCP宛パケットは継続的に観測している.

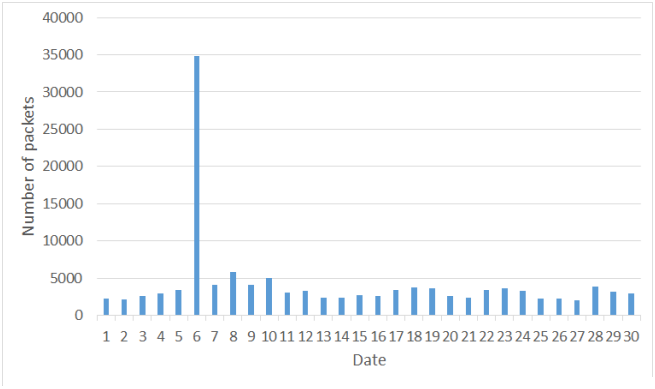

図 1. 2015 年 11 月のダークネット宛 ポート 6000/TCP へのパケット数

表 1. 2015 年 11 月 6 日のポート 6000/TCP へのパケット送信数と送信元 IP アドレス(上位 5 件)

送信元 IP アドレス	パケット数	割合(%)
A	30,786	88.4
B	561	1.6
C	366	1.1
D	357	1.0
E	327	0.9
全体	34,827	100

なおホスト A から同ポートへ宛てたパケットは, 11 月 6 日を除いて本調査期間中には観測しておらず, このパケット増加の原因は脆弱性の公表を見た悪意あるユーザが, 修正パッチを未適用の該当サーバを探索する目的で送信したパケットだと推測できる. ソフトウェアの利用者は脆弱性が公表されてから即時に修正パッチを適用できるとは限らない為, これもゼロデイ攻撃にあたるが, 未知の脆弱性を標的とした攻撃を検知するには, 脆弱性が公表される前の挙動の変化の事例が必要となる. ダークネット観測によってゼロデイ攻撃を把握するにはさらなる攻撃の事例を発見する必要がある.

4 まとめと今後の課題

ダークネット宛のトラフィックデータを解析した結果, 脆弱性が報告されたソフトウェアの用いるポートへのパケット数が顕著に増加していた. しかしこれらは脆弱性が公表された後での変動であり, 未知の脆弱性に対するゼロデイ攻撃の把握には, 脆弱性発覚前での挙動の変化事例が必要となる. 今後はログの解析をさらに進めて他のゼロデイ攻撃の痕跡を調査するとともに, ゼロデイ攻撃の特徴がどのようにダークネット上に表れるかを分析していき, ダークネット通信を解析することがゼロデイ攻撃の把握に有用かどうか, 引き続き検証していく.

参考文献

[1] Common Vulnerabilities and Exposures, https://cve.mitre.org/
[2] AbuseIPDB https://www.abuseipdb.com/