一般口演 | 病院情報システム
一般口演12
病院情報システム
2019年11月23日(土) 09:00 ～ 11:00 F会場 (国際会議場 3階中会議室302)

[3-F-1-06] 医療機関の情報ネットワークに対する外部からの不正アクセスに関する分析～ゼロデイ攻撃は行われたのか～

○松永 敏明[1]、矢野 弘章[1]、三浦 亜耶乃[1]、難波 孝宏[1]、森 龍太郎[2]、青木 光広[2]（1. 岐阜大学医学部附属病院　経営企画課　医療情報係, 2. 岐阜大学医学部附属病院　医療情報部）

キーワード：Network, Hospital Information System, Unauthorized access

【背景と目的】医療機関の情報ネットワークはその特性上、安定稼働が最優先される。しかし、扱う情報は重要度の高い要配慮個人情報であるため高いセキュリティで守られることが求められている。

　一方、 Windows7のサポート終了を来年2020年1月14日に控えた昨今、5月14日にマイクロソフトよりリモートデスクトップサービスのリモートでコードが実行される脆弱性（ CVE-2019-0708）が報告され、脆弱性を狙った不正アクセスが増加すると考えられる。

本稿では院内ネットワークと院外ネットワークの境界線に設置した UTM（統合脅威管理）で遮断した外部からの不正アクセス通信ログを解析し、医療機関に対する不正アクセスの傾向について解析した。

【解析方法】 UTMから取得した、2017年6月から2019年5月の間のログ情報（約180万件）より、リモートデスクトップサービスの通信ポート（ポート番号：3389）で不正アクセスを試みた数の推移やその傾向等について解析した。

【結果】月別での不正アクセスの件数は増加傾向にある中で、2019年5月の件数は突出していた。その月にフォーカスを当て、日別での不正アクセスの件数はそれ以前の日に比べ5月13日から1.5倍に増加していた。5月14日の発表より先に脆弱性の情報を入手していち早く不正アクセスを試みたのではないかと考えられ、ゼロデイ攻撃が行われたといえる。

【考察】日々脆弱性等の情報が提供される中、検証に時間をかける、周囲の動きを見てから行動を起こすといったことがよく聞かれるが、攻撃者はそれを待つことなく攻撃は行われる。 AI等の新たな技術が早いスピードで取入れられるのと同じように、情報セキュリティ対策でも迅速な対応が求められる。

医療機関の情報ネットワークに対する外部からの不正アクセスに関する分析
－ ゼロデイ攻撃は行われたのか －

松永　敏明[*1]、矢野　弘章[*1]、三浦　亜耶乃[*1]、難波　孝宏[*1]、
森　龍太郎[*2]、青木　光広[*2]
*1 岐阜大学医学部附属病院　経営企画課　医療情報係、
*2 岐阜大学医学部附属病院　医療情報部

An analysis of the unauthorized outside access of an information network at a medical institution
- Was the zero-day attack done -

Toshiaki Matsunaga [*1], Hiroaki Yano[*1], Ayano Miura[*1], Takahiro Nanba[*1],
Ryutaro Mori[*2], Mitsuhiro Aoki[*2]
*1 Management Planning Division, Gifu University Hospital,
*2 Medical Information Department, Gifu University Hospital

We analyzed the tendency of unauthorized access in our hospital.This time Microsoft reported a vulnerability in the remote desktop service.Based on this information, a zero-day attack was conducted.Currently, unauthorized access threatens information security not only in medical institutions but also in general society.Unauthorized attempts for unauthorized access are increasing year by year, and the techniques are becoming more complex, so more advanced security measures must be taken.

Keywords: Network, Hospital Information System, Unauthorized access.

1. 緒論・目的

医療機関の情報ネットワークはその特性上、安定稼働が優先される。しかし、扱う情報は重要度の高い要配慮個人情報であるため高いセキュリティで守られることが求められている。

一方、Windows7 のサポート終了を来年 2020 年 1 月 14 日に控えた昨今、2019 年 5 月 14 日と 8 月 13 日にマイクロソフトよりリモートデスクトップサービスのリモートでコードが実行される脆弱性(CVE-2019-0708,CVE-2019-1181)が報告され、脆弱性を狙った不正アクセスが増加すると考えられる。

本稿では院内ネットワークと院外ネットワークの境界線に配置した UTM(統合脅威管理)で遮断した外部アクセス通信ログを解析し、医療機関に対する不正アクセスの傾向について解析した。

2. 方法

外部ネットワークから岐阜大学医学部附属病院（以下、本院と言う。）で運用している外部公開用サーバに対して行われた不正アクセスの試みについて、UTM から取得した 2017 年 6 月から 2019 年 8 月の間のログ情報(約 250 万件)より、不正アクセスを試みた数の推移やその傾向などについて解析を行った。

3. 結果・考察

3. 1 月別傾向解析

月別不正アクセスの傾向を図1に示す。

各年の 6 月を比較すると、2017 年は 49,122 件、2018 年は 73,146 件、2019 年は 99,259 件で、2017 年から 2018 年が 1.48 倍に、2018 年から 2019 年が 1.35 倍に増加していた。その他の月でも増減のばらつきはあるが、全体的に増加の傾向があると言える。2017 年 6 月と 2019 年 8 月を比較すると 49,122 件から 136,110 件へと約 2.8 倍に増加していた。

全体的に増加な傾向の中、2018 年 2 月と 2019 年 7 月が他の月に比べ突出していた。

2018 年 2 月は 92,426 件であった。前月の 55,296 件に対して約 1.7 倍の件数が確認された。これは 2 月 14 日にブルガリアから 34,556 個のポートに対する不正アクセスであり、多くのポートに各 1 回ずつの不正アクセスを試みていることからポートスキャンが行われたと考えられる。

2019 年 7 月は 427,934 件であった。前月の 99,259 件に対して約 4.3 倍の件数が確認された。これは日本のある IP アドレスから 10,974 個のポートに 15 日間かけて各ポートに 2 回ずつで総計 315,808 件の不正アクセスを試みていた。

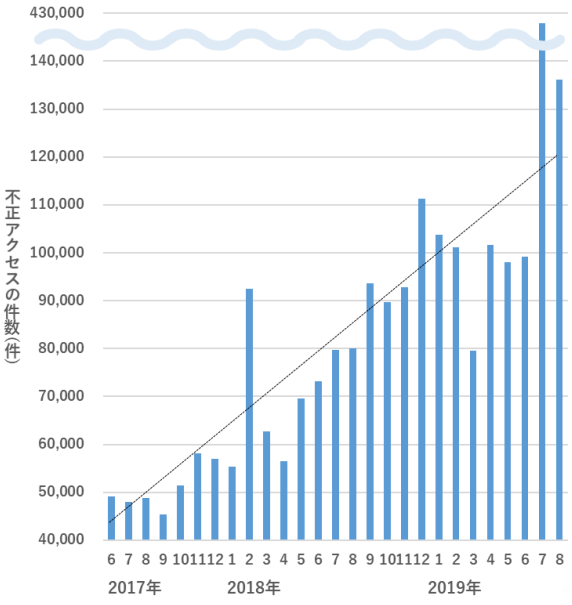

図1　月別不正アクセスの傾向

3.2 リモートデスクトップサービスの通信ポートの傾向解析

リモートデスクトップサービスの通信ポート(ポート番号:3389)による月別不正アクセスの傾向を図2に示す。

マイクロソフトよりリモートデスクトップサービスの脆弱性が報告されたが、その影響が見られるか解析を行った。

2017 年 6 月と 2019 年 6 月を比較すると 668 件から 1,119 件へと約 1.7 倍に増加していた。月別の傾向と同じように全体的に増加の傾向があると言える。月により増減のばらつきがある中一定の範囲内で推移していたが、2019 年 5 月以降は 5 月が 1,378 件、7 月が 1,279 件、8 月が 1,290 件と一定の範囲を超える件数があった。

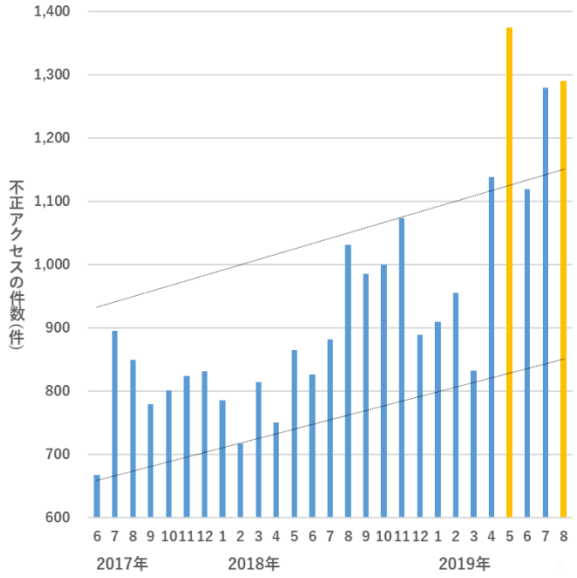

図2 リモートデスクトップサービスの通信ポートの月別不正アクセスの傾向

3.3 2019 年 4 月から 8 月のリモートデスクトップサービスの通信ポートの傾向解析

2019 年 4 月から 8 月のリモートデスクトップサービスの通信ポートによる日別不正アクセスの傾向を図3に示す。

図3でマイクロソフトより脆弱性が報告された 5 月 14 日と 8 月 13 日を別色に変えた。

日により不正アクセスの件数は前後しているが、5 月 14 日近辺では前日の 5 月 13 日から 5 月 24 日まで 50 件を超える日は 9 日間あった。また、8 月 13 日から 8 月 17 日まででは 4 日間あった。

2017 年 6 月から 2019 年 5 月 12 日までの約 2 年間で 50 件を超える日は 5 日間であった。その一方 5 月 13 日以降の 3 ヶ月半で 23 日間であった。

これは脆弱性の情報を元に不正アクセスを試みたと考えられ、ゼロデイ攻撃が行われたと言える。

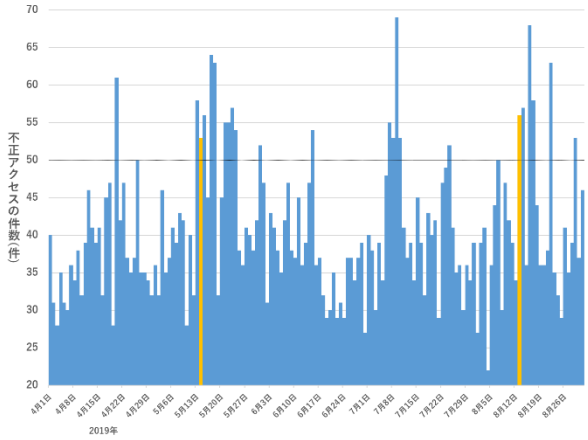

図3 2019 年 4 月から 8 月のリモートデスクトップサービスの通信ポートの日別アクセスの傾向

3.4 IP 別傾向解析

IP 別不正アクセスの傾向を表1に示す。

表1では不正アクセスの攻撃元の IP アドレスと国名と不正アクセスの件数で上位 10 件を示す。

この IP アドレスや国名は UTM のログで取得できた値のため、偽装されている可能性はある。また、IP アドレスも分散させている可能性もある。

上位 10 件のうち国名だけ見ても日本と中国とオランダが占めていた。

114.156.2.66 は 2019 年 7 月の 15 日間、85.93.20.245 は 2018 年 2 月 14 日の 1 日間で表の件数の不正アクセスを試みていた。この 2 つは複数のポートへの不正アクセスを試みるポートスキャンを行っていた。

一方、221.228.97.218 はポート番号 53413 番のみをほぼ毎日様々な時間に不正アクセスを試みていた。ポート番号 53413 番は中国の Netcore(中国国内)/Netis(中国国外)社製ルータで利用され、このルータの脆弱性を利用すると、ルータをほぼ完全に制御される可能性がある。

同様に各 IP アドレスからの不正アドレスは上記のように、特定日に複数ポート番号への不正アクセスを試みる場合と、継続的に指定ポート番号への不正アクセスを試みる場合があった。

表1 IP 別不正アクセスの傾向

IP アドレス	国名	件数
114.156.2.66	Japan	315,808
85.93.20.245	Bulgaria	35,243
221.228.97.218	China	15,965
153.139.227.114	Japan	11,259
223.105.4.245	China	8,115
114.156.2.74	Japan	7,570
185.208.208.198	Netherlands	7,148
120.197.97.27	China	7,096
185.208.209.6	Netherlands	6,137
191.101.167.30	Netherlands	5,658

4. 結論

本稿では本院における不正アクセスの傾向について解析を行った。現在は医療機関に限らず社会一般で不正アクセスは情報セキュリティを脅かしている。年々不正アクセスの試みは増加しており、手口も複雑化しているためより高度なセキュリティ対策を行わなければならない。

今回のマイクロソフトよりリモートデスクトップサービスの脆弱性が報告された。その情報を元にゼロデイ攻撃が行われた言える結果となった。

リモートデスクトップは遠隔地からコンピュータを操作できる便利な機能であり、リモートデスクトップサービスは Windows の標準機能として搭載されているため、利用しやすい機能ではある。

しかし、VNC(Virtual Network Computing)等のソフトウェアが充実している中、リモートデスクトップサービスにこだわる必要はない。

ただ、今でもリモートデスクトップサービスのポートを開放してほしいと院内・院外・ベンダーから要求される。他の機能を提案してもリモートデスクトップサービスでしか対応できないとの回答もあった。難しい技術力を必要とするわけではないため対応してもらいたい。