アンラボ・セキュリティレター

Press Ahn

2016.5　Vol.29

ランサムウェアが医療機関を狙う

標的型攻撃に進化中のランサムウェア

ランサムウェアが医療機関を狙う

不特定多数を対象に攻撃を仕掛けていたランサムウェアだが、最近はターゲットに狙いを定めた攻撃に様相が変化し、その手法も高度化している。特に今年に入り医療機関を中心にランサムウェアの被害ケースが多く報告されている。患者の命と直結する重要情報が多いため、医療機関のランサムウェア脅迫に対する反応率はその他産業に比べて非常に高いほうだ。今回のコラムでは医療機関で発生したランサムウェアのケースを紹介し、その対策を講じる。

医療機関を狙うランサムウェア登場

今年 3月、アメリカの大型病院からランサムウェア被害が報告された。被害にあった病院は Methodist Hospital、Chino Valley Medical Center、Desert Valley Hospitalの3箇所だった。またこれらの病院に先立ち Hollywood Presbyterian Medical Centerでもランサムウェアに感染されていたことが分かった。Hollywood Presbyterian Medical Centerは、ランサムウェアによって十日間システムアクセスが不能になり、結局攻撃者に身代金(1万7千ドル)を支払ってから復元させたという。

[図1] Methodist Hospitalサイトの上段バナーに『マルウェア感染によるサービス使用制限のお知らせ』と表示されている

従来のランサムウェアは不特定多数を狙う無差別攻撃を仕掛けていたが、最近はターゲットを定めて攻撃する標的型ランサムウェアに進化している。2015年末には医療機関をターゲットにしたランサムウェア『SamSam』が登場した。通常のランサムウェアはスパムメールや脆弱なサイトから不特定多数に向けて大量にマルウェアを配布し、感染されたユーザー PCのファイルを暗号化してから USDあるいはビットコイン(Bitcoin)を要求する。だが SamSamは、特定グループ内で使用するインフラに脆弱性があるかどうか探り、そこから内部及びネットワークで繋がるユーザー PCのファイルを暗号化しては、金銭を要求する手法をとっている。同マルウェアは、攻撃者がアップロードした RSAキーを実行してシステムを感染させ、重要な文書及び画像ファイルを RSA-2048方式で暗号化し、データを人質にしたことを通知する HTMLを作成する。

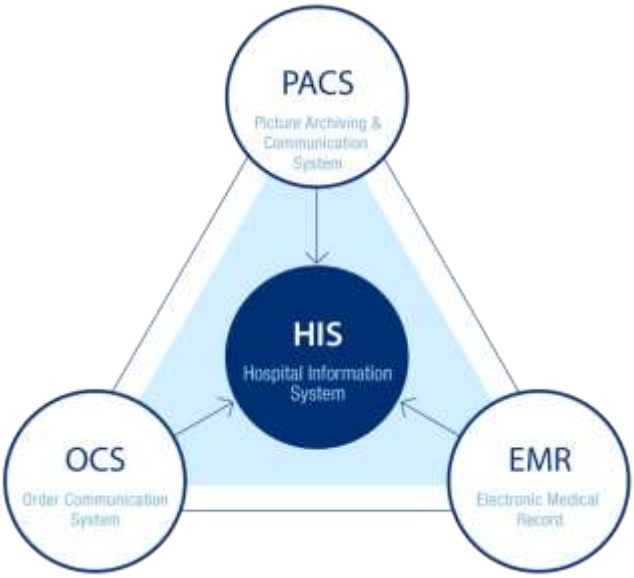
[図2] 暗号化したことをユーザーに通知する HTML

アンラボの製品では、ランサムウェア『SamSam』を次のような診断名で検知している。

V3 製品群の診断名	Trojan/Win32.Samas
AhnLab MDS 診断名	Suspicious/MDP.Create、 Malware/MDP.Behavior

病院情報システム(HIS)と潜在的脅威

ほとんどの医療機関では医療及び行政手続きを管理するための「病院情報システム(Hospital Information System, 以下 HIS)」を使用している。これは診療状況から医薬品管理、財務管理、患者管理及び各種の医療画像情報まで管理する統合システムだ。特に HISの中核といえる電子カルテ(Electronic Medical Record, EMR)、処方管理システム(Order Communication System, OCS)、医療用画像管理システム(Picture Archiving & Communication System, PACS)は、ネットワークで繋がるシステム同士有機的に連動し、重要な患者情報を扱っている。

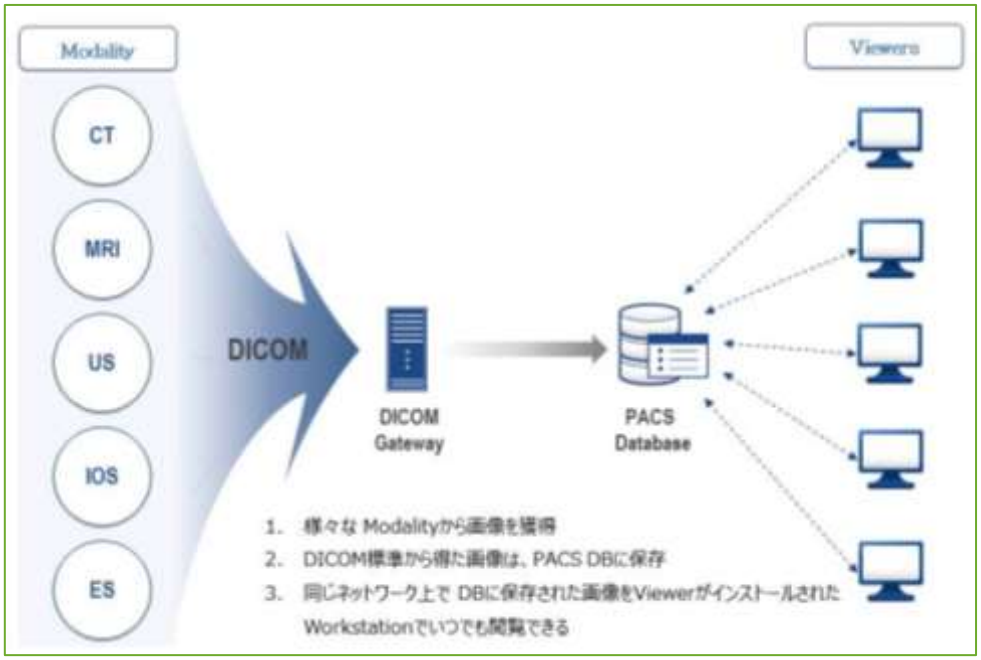


[図3] 主要な病院情報システム

その中で PACSは、多様な医療用画像装置(MRI, CT, X-rayなど)から得られた画像情報を保存及び送信する領域で使用され、患者の治療及び生命とも直結する非常に重要な情報システムだ。

また韓国は医療画像及びそのカルテの法的義務保管期間が 5年であるため、資料のバックアップ管理も重要になってくる。

もし NAS(Network Attached Storage)領域に保存された PACSのデータが、画像判読ビューアーがインストールされたクライアント端末に侵入したランサムウェアによって暗号化されたうえ、同じネットワーク上に位置するルートに保存されたバックアップデータまで暗号化されてしまったら、病院のセキュリティ担当者としては想像もしたくない事態が発生するだろう。



* CT(Computed Tomography), MRI(Magnetic Resonance Imaging), US(Ultrasound), DR(Digital Radiography), ES(Endoscopy)

[図4] PACSシステム概念図

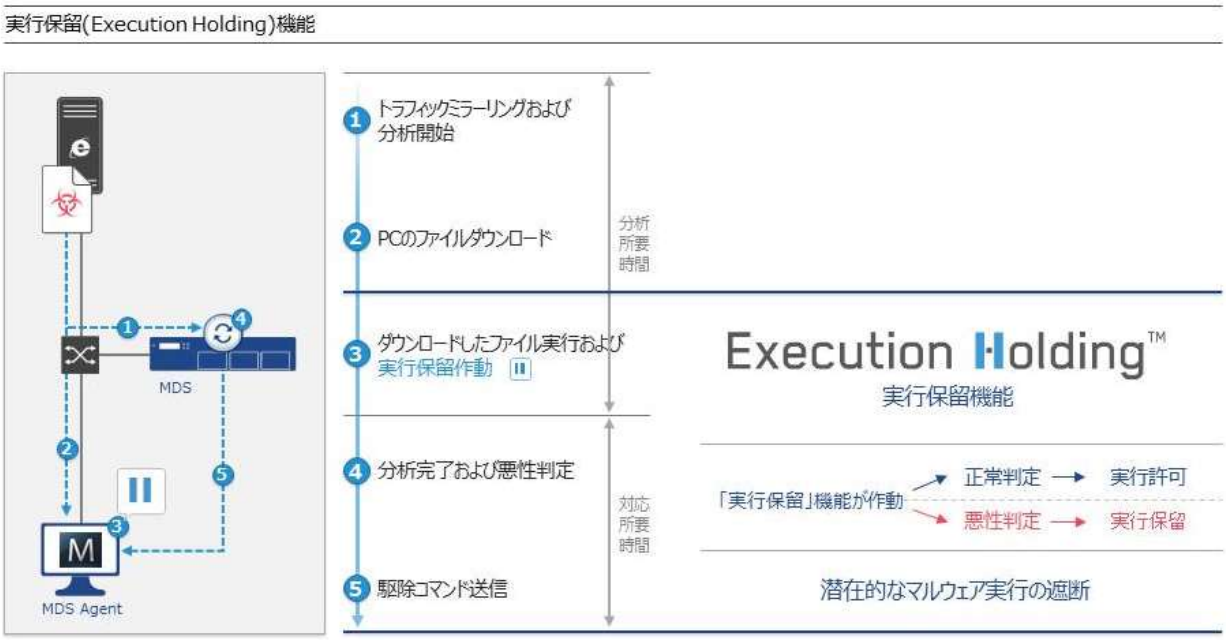
PACSサーバーに保存される医療画像情報は、米国放射線科医学会(A.C.R)と米国電機工業会(NEMA)で構成された連合委員会で決めた医療用画像標準の『DICOM(Digital Imaging & Communications in Medicine)ファイル形式』で保存・管理される。これは単なる画像ではなく、データ送信(Transfer)、保存(Storage)及び出力(Display)に対する全般的な標準だ。標準に則り該当の画像には DICOMタグ(Tag)情報が付けられ、ここには患者の性別・年齢・氏名などの個人情報が含まれる。もしランサムウェアに感染して暗号化された後、これらの情報が流出されてしまい復号キーとともにブラックマーケットで販売でもされれば大事件になる。最近大ヒットした韓国ドラマ「太陽の末裔」でも、国の要人の医療情報が機密情報として扱われるシーンがあった。医療情報が悪意ある目的をもって流出されたら深刻な事態に陥るだろう。

[図5] DICOM Viewerで写し出された画像(左)とDICOM Tagに付けられる各種情報(右)

* 出典: http://www.codeproject.com/Articles/36014/DICOM-Image-Viewer

進化するランサムウェアに対抗する

マルウェア作成者をはじめとするサイバー犯罪者らは、セキュリティソリューションを回避するランサムウェアの変種を着実に拡げている。そして配布の拡散に止まらず、金銭的利得を最大化するための特定の標的を狙う攻撃手法へとシフトさせているのだ。アンラボは持続的に進化するランサムウェアに対応するため、多様な変種に関する診断を持続的に追加している。またインテリジェンスな脅威対応ソリューション「AhnLab MDS」の「実行保留機能(Execution Holding)」により、従来のランサムウェアだけでなく多様な変種への対応も可能になった。特徴としては、ユーザーが認知できない状態でマルウェアが自動でインストールされるダウンロード実行(Drive-by-Download)手法の被害を防止できる。



[図6] AhnLab MDS 実行保留(Execution Holding)機能

AhnLab MDSの対ランサムウェアの鍵は「実行保留機能」だ。同機能はネットワーク上で検知された疑わしいファイルの分析が終了する前に、該当のファイルが実行されることを保留して分析後、正常ファイルと判定されたファイルのみ実行させる。

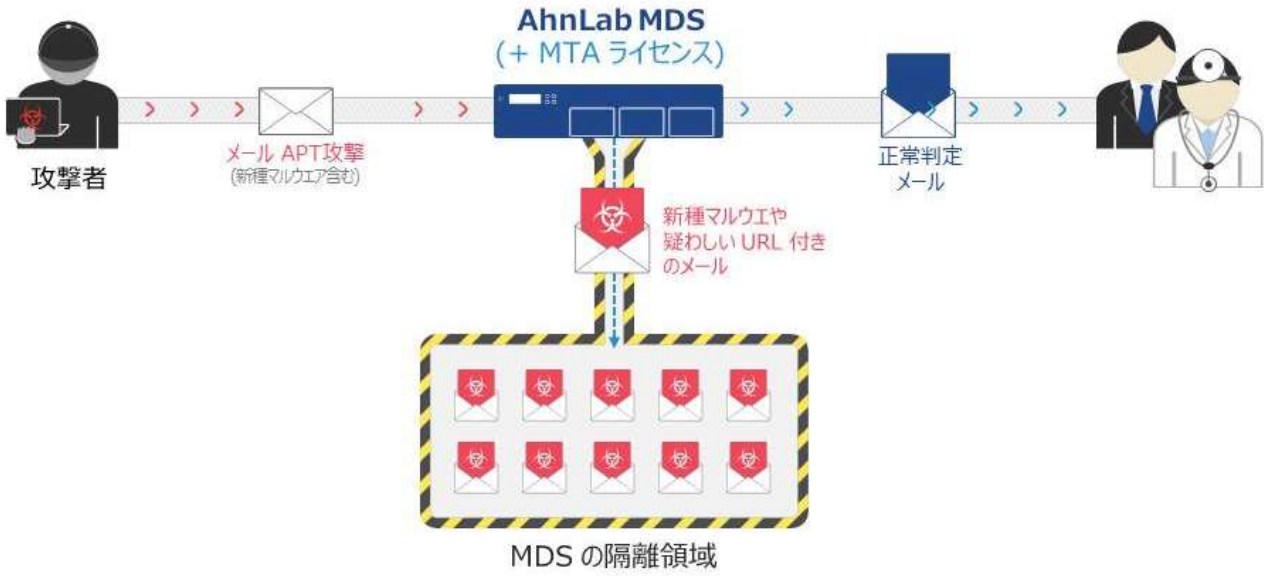
ランサムウェア SamSamもサーバーの脆弱性を突いて侵入し、トリガー(Trigger)タイプの悪意あるファイルをローカルネットワーク端末で実行させるタイプだ。この時 MDSの実行保留機能があれば、侵入したランサムウェアがローカルのファイルを暗号化する動作を防止できる。

標的型に進化中のランサムウェアは、主にスピアフィッシング(Spear Phishing)手法を利用する。スピアフィッシングはスパムメールとは異なり、特定の組織を狙う標的性と、正常なファイルやメールに見せかける精巧なテクニックを併せ持つ。MDSはスピアフィッシング手法で配布されるメールに対応するため、電子メール隔離(MTA)機能も提供している。これはマルウェアが添付されていたり、疑わしい URLが含まれたメールを MDSのスペシャルエリアに隔離させる機能だ。

ますます高度化する脅威に対抗するためにはセキュリティの 3大要素「人」、「技術」、「プロセス」の調和が求められる。まずは現在発生している脅威から大事な情報を守るため、技術的なアプローチによるソリューションの導入が必要だ。

MDSが提供する電子メール隔離(MTA)機能で、悪意あるメール(マルウェア入り添付ファイル及びメール本文に悪質なURLが含まれたメール)を隔離すればスピアフィッシング攻撃を事前に防ぐことができる。

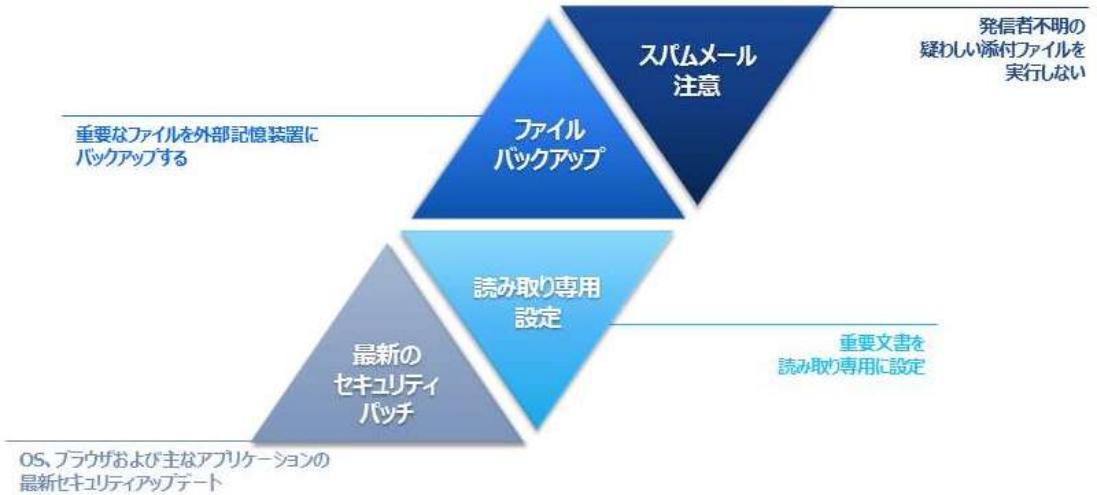
また実行保留機能が作動して「実行を保留された疑わしいファイル」が最終的に悪性判定を受けると、該当ファイルを削除・隔離する。これにより、ユーザーのシステム環境を安全に保護できる。特に文書型マルウェア分析に最適化された「動的コンテンツ分析技術(Dynamic Intelligent Content Analysis, DICA)」なら、疑わしい行為の有無に関係なく文書アプリケーションのゼロデイ脆弱性まで正確に把握できる。



[図7] AhnLab MDS電子メール隔離(MTA)機能

終わりなき戦い

昨今医療機関とヘルスケア分野への攻撃は持続的に発生し、対策として多くのガイドラインが政府や公共機関から配布されている。ここまで紹介したほとんどの事例では、暗号化を解くために支払った身代金の被害規模のみが注目されていた。だがもっと広い視野でみれば病院システムがランサムウェアに人質にされた期間中、医療機関が被った定量的な収益減少と患者への被害、そして病院イメージの打撃も見過ごせない深刻なダメージなのである。



[図 8] ランサムウェア予防のためのセキュリティガイドライン

対ランサムウェアのために重要なのは人とプロセスの整備だ。組織の中で、利便性のためにセキュリティが蔑ろにされているプロセスはないか点検し、セキュリティをベースにした業務プロセスの確立が必須となる。そして従業員のセキュリティへの認識改善教育と、基本的なランサムウェア予防ガイドに関する持続的な教育も並行されることが望ましい。

[参考文献]

[1] CYBERATTACKERS DEMAND $3.6M RANSOM FROM HOLLYWOOD HOSPITAL
(http://www.hipaajournal.com/cyberattackers-demand-3-6m-ransom-from-hollywood-hospital-8313/)

[2] As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up $17,000 In Bitcoin
(http://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#1dff2c6b75b0)

[3] Hollywood Hospital Victimized by Ransomware Locky Spreading Fast
(http://www.ktvn.com/story/31274059/hollywood-hospital-victimized-by-ransomware-locky-spreading-fast)

[4] A Hospital Paralyzed by Hackers
(http://www.theatlantic.com/technology/archive/2016/02/hackers-are-holding-a-hospitals-patient-data-ransom/463008/)

[5] このランサムウェアは医療機関のみ狙う (http://techholic.co.kr/archives/51555)

[6] 1週間で3箇所の病院がランサムウェアに！医療業界の危機 (http://www.boannews.com/media/view.asp idx=50052&kind=4)

[7] 主要医療機関のランサムウェア対応状況を緊急診断 (http://www.boannews.com/media/view.asp idx=50174)

[8] ランサムウェアの人質にされた米国の病院、最終的に1万7,000ドルを支払う
(http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do menu_dist=1&seq=24661)

[9] SAMSAM: THE DOCTOR WILL SEE YOU, AFTER HE PAYS THE RANSOM (http://blog.talosintel.com/2016/03/samsam-ransomware.html m=1)

[10] Check Point Threat Alert: SamSam and Maktub Ransomware Evolution
(http://blog.checkpoint.com/2016/03/28/check-point-threat-alert-samsam-and-maktub-ransomware-evolution/)

[11] 医療機関サーバーの脆弱性を狙う「SamSam」と、感染拡散のためにファイルを圧縮する「Maktub」発見
(http://www.boannews.com/media/view.asp idx=50117&skind=O)

[12] SamSamランサムウェア、特定の組織を狙う標的型に進化 (http://www.boannews.com/media/view.asp idx=50198)

[13] Samsam may signal a new trend of targeted ransomware
(http://www.symantec.com/connect/blogs/samsam-may-signal-new-trend-targeted-ransomware)

[14] No mas, Samas: What's in this ransomware's modus operandi?
(https://blogs.technet.microsoft.com/mmpc/2016/03/17/no-mas-samas-whats-in-this-ransomwares-modus-operandi/)

[15] Evolution of SamSa Malware Suggests New Ransomware Tactics In Play
(http://researchcenter.paloaltonetworks.com/2016/03/evolution-of-samsa-malware-suggests-new-ransomware-tactics-in-play/)

[16] DICOM Standard (http://dicom.nema.org/standard.html)

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)