TLP : AMBER

セキュリティインシデント解析事例

インターネットに接続された OT 環境で発生したランサムウェア感染

AhnLab SEcurity intelligence Center (ASEC)

2024.07.03

AhnLab

ドキュメントレベルについてのご案内

刊行物や提供されるコンテンツは、以下のようにドキュメントレベルごとに許可された範囲内でのみ使用可能です。

ドキュメントレベル	配布対象	注意事項
TLP ： RED	特定のクライアントにのみ提供されるレポート	**レポートの受信者もしくは受信部署でのみ閲覧可能なドキュメント** 受信者以外への複製・配布不可
TLP ： AMBER+STRICT	限られたクライアントにのみ提供されるレポート	**レポート受信組織（会社）内部では複製・配布可能** ただし、組織外での教育目的などで使用する場合はアンラボの許可が必須
TLP ： AMBER	限られたクライアントおよびクライアントの顧客にのみ提供されるレポート	**レポート受信組織（会社）内部および当該組織の顧客では複製・配布可能** ただし、対象者外の教育目的などで使用する場合はアンラボの許可が必須
TLP ： GREEN	コミュニティ内の誰でも利用可能なレポート	**その業種などで自由に使用でき、出典を明記する場合は内部教育、同種業界、セキュリティ担当者教育資料として活用可能** ただし、一般ユーザーを対象とした発表資料としては厳しい制限あり
TLP ： CLEAN	自由に利用可能なレポート	出典明記 商業性の有無にかかわらず利用可能 変形など 2 次的著作物の作成可能

目次

解析概要 4
事例からの教訓 5
解析の詳細 5
一般的な OT 環境について 5
IT 環境と OT 環境の違い 5
OT セキュリティの構成 6
被害システムの OT 環境構成 9
侵害フロー図 9
インターネットに接続された閉域網 9
管理者アカウントのログオンが発生 10
ラテラルムーブメント 10
検知の回避 11
ランサムウェア感染 12
MITRE ATT&CK 13
Threat Hunting Rules 15
IoC (Indicators of Compromise) 16
不正ファイル 16

CAUTION

本レポートには現在までに確認された内容に基づいて分析者の意見が多く含まれています。
分析者ごとに意見が異なる場合があり、新たな根拠が確認される場合、
本レポートの内容が事前告知なしに変更される可能性があります。

解析概要

ASEC (AhnLab SEcurity intelligence Center) は、OT (Operational Technology) 環境で発生したランサムウェア感染事例を確認した。OT 環境は、インフラストラクチャー、製造業などの運用技術に重点を置いた分野であり、設備および機器のタイプによってネットワークを区分し、断絶された閉域網環境で運用される。

従来の OT 環境で発生したセキュリティインシデントの事例は、内部の閉域網を侵害するために外部ネットワークから内部閉域網まで、緻密に準備された APT 攻撃によるものとして知られてきた。しかし、今回の事例は論理的なネットワーク分離により運用されている OT 環境において、生産設備のメンテナンスのために閉域網に直接インターネットを接続したことで問題が発生した。

OT 環境を直接狙った APT 攻撃ではなかったが、不適切なネットワーク接続により外部インターネットに生産設備の資産がさらされ、ランサムウェアに感染して生産ラインが停止する被害が発生した。生産設備には同じメーカーの設備が多数存在し、メーカーの初期パスワードをそのまま使用していた設備により、さらに大きな被害へとつながった。

区分	内容
攻撃者	● Phobos
主な攻撃内容	● ランサムウェア感染
被害状況	● ランサムウェア感染による生産設備の障害発生
被害環境	Windows 10
事例 TAG	#Phobos #ransomware #lateralmovement #RDP #windowsdefender #netpass #dcontrol #OT

表1. 解析サマリー

事例からの教訓

問題点	対応策
● 閉域網環境へのインターネット接続により、内部システムがインターネット上にさらされる	● 例外状況（システムメンテナンス）が増加するほど、閉域網環境への攻撃ベクトルが増加することに注意 ● 閉域網のインターネット接続制限、インターネット接続なしでメンテナンスを実施できる案を優先的に考慮
● 閉域網環境内の資産が脆弱な状態（セキュリティアップデートの未実施、セキュリティプログラムの未インストール）で管理されている	● セキュリティプログラムのインストール ● 最新のセキュリティアップデートを適用
● 製品名で登録されたシステム名と、初期パスワードの使用による侵害が発生	● システムを推測されにくいシステム名に変更 ● 製品の初期パスワードは必ず変更してから使用

解析の詳細

一般的な OT 環境について

IT 環境と OT 環境の違い

OT 環境とは? OT (Operational Technology) 環境は産業の運用技術環境であり、産業用制御システム (ICS: Industrial Control System) だけでなく、IT と接続、または同時に使用される広範囲の領域を意味します。

IT (Information Technology) はデータの処理および送信を主な目的として、「情報」に重点を置く技術であり、OT (Operational Technology) は物理的設備をモニタリングして制御する、「運用」に重点を置く技術といえる。

IT 技術と OT 技術が違うように、IT セキュリティと OT セキュリティにも違いが存在する。情報セキュリティの 3大要素と言われる機密性 (Confidentiality)、完全性 (Integrity)、可用性 (Availability) においても、IT は機密性、完全性、可用性の順に重要度を評価している。OT セキュリティでは IT セキュリティと違って、可用性、完全性、機密性の順に重要度を評価している。

例えば、IT 環境では資産 (PC、ノートパソコン、モバイル、サーバーなど) に問題が発生したとき、問題解決のために再起動、資産の入れ替え措置が可能である。しかし、OT 環境では資産の再起動、入れ替えなどの措置は生産設備の中断につながるため、機密性よりも可用性と完全性をより高く評価している。

IT セキュリティの セキュリティ要素における優先順位	OT セキュリティの セキュリティ要素における優先順位
1. 機密性 (Confidentiality) 2. 完全性 (Integrity) 3. 可用性 (Availability)	1. 可用性 (Availability) 2. 完全性 (Integrity) 3. 機密性 (Confidentiality)

表2. IT セキュリティと OT セキュリティの情報セキュリティ 3大要素における優先順位

OT セキュリティの構成

一般的に OT セキュリティを説明するときは「Purdue モデル」を利用してネットワークセキュリティの階層を説明する。Purdue モデルは、ネットワーク環境を Level 0 から Level 5 まで、6つの階層で区分している。6つの階層には IT 環境を意味する Level 4/5 のインターネット環境と、OT 環境を意味する Level 0 から Level 3 までの閉域網環境がある。OT 環境についても、制御ネットワーク (Level 0～Level 2) と運用ネットワーク (Level 3～Level 3.5) で区分して考える場合もある。

だが、生産設備が実際に稼働している現場では、Purdue モデルのような形でネットワークが区分されていないか、ネットワークは区分されていても脆弱な管理体制により侵害が発生する場合がある。

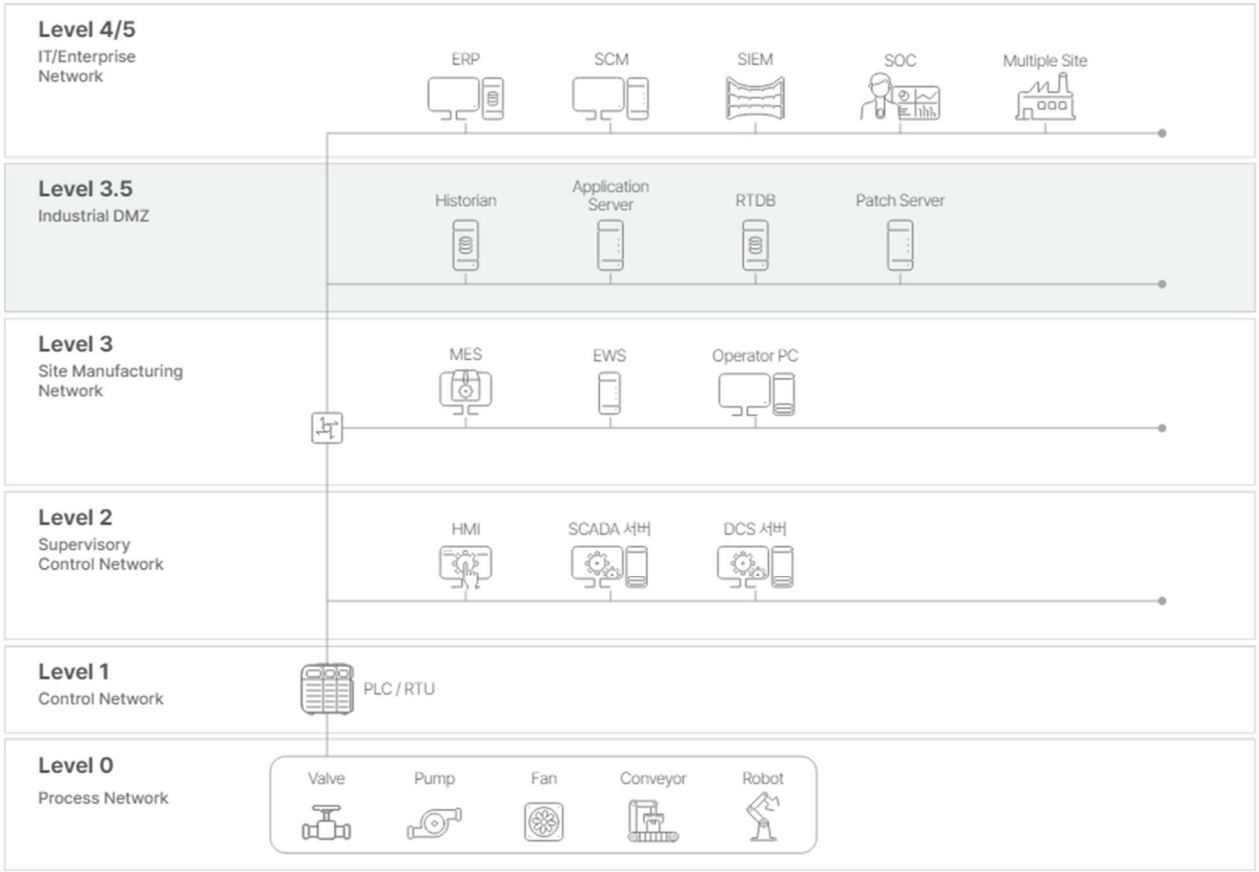


図1.Purdue モデル (Purdue Model)

OT 環境で発生するセキュリティインシデントは Level 4/5 の IT ネットワークから始まるケースが多い。IT ネットワークの侵害により、内部ネットワーク構造がさらされる場合がある。閉域網で運用される OT ネットワークの侵害は、管理が不適切なアクセス制御ポリシー、外部と接続された OT ネットワーク、または不適切な記録メディアの使用などにより発生することがある。OT ネットワークの老朽化したシステムと管理状態が脆弱なシステムは、内部に流入したマルウェアに感染して被害を受ける場合がある。

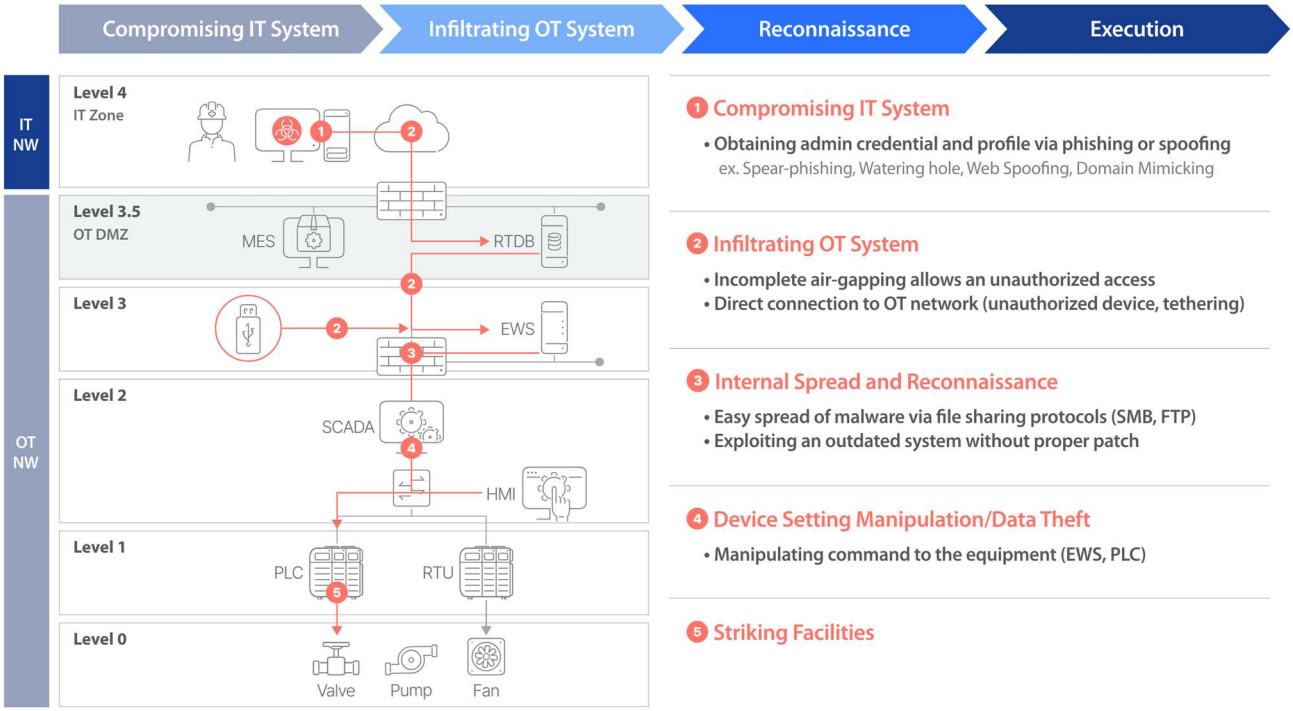


図2. OT 環境の侵害フローの例

アンラボでは、OT 環境のセキュリティに対する重要性を認知しており、OT セキュリティの詳細についてはアンラボが発行した「OT 環境でも統合セキュリティが必要な理由」で確認することができる。[1]

[1]https://www.ahnlab.com/jp/contents

被害システムの OT 環境構成

侵害フロー図

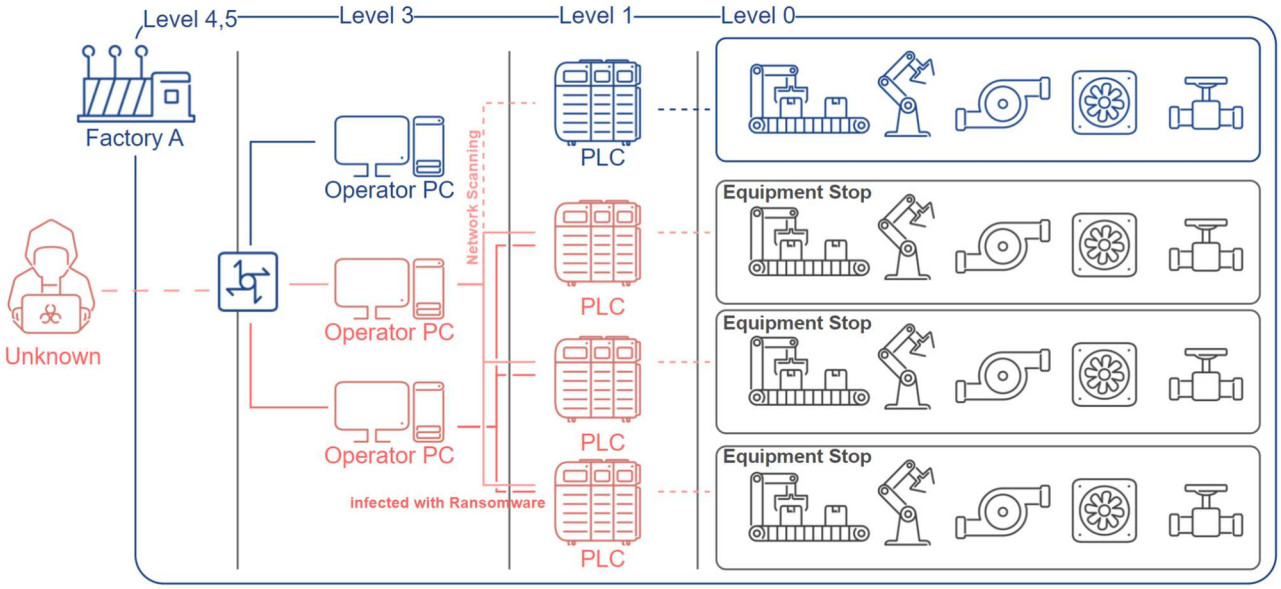


図3. 侵害フロー図

インターネットに接続された閉域網

OT 環境内の生産設備を統制するシステムのメンテナンス過程で、ランサムウェアによる侵害が発生した。システムメンテナンス中に外部インターネットに接続し、それによって OT 環境の資産がインターネット環境にさらされ、ランサムウェアによる感染被害へとつながった。

OT 環境は閉域網で構成されたが、論理的なネットワーク分離であったため、運用システムのメンテナンスのためのインターネット接続が可能だった。管理者は侵害の時点で論理的なネットワーク分離が適用されたルーターに外部インターネットに接続可能なネットワーク帯域を設定した。その後、インターネットが可能なネットワーク帯域を内部運用システムに順次割り当てながらメンテナンスを実施した。

メンテナンスの実施中、運用システムは外部インターネット網にさらされ、運用システムの中にはセキュリティプ

ログラムのインストールが不十分、またはセキュリティアップデートを適用していないなど、脆弱な状態で管理されているシステムが存在した。

管理者アカウントのログオンが発生

An account was successfully logged on.

Subject:

Security ID:	S-1-5-18
Account Name:	[redacted]
Account Domain:	WORKGROUP
Logon ID:	0x3e7

Logon Information:

Logon Type:	10
Restricted Admin Mode:	아니요
Virtual Account:	아니요
Elevated Token:	예

図4. Administrator アカウントでログオンしたイベントログ

外部にさらされた運用システムは、管理者アカウントである Administrator に対するログオン攻撃の試みを受けた。このうち、脆弱なパスワードで管理されていた運用システムが侵害を受けた。侵害されたシステムはその後、内部ネットワーク帯域でのスキャン攻撃が実行された。

ラテラルムーブメント

運用 PC が侵害されたあと、攻撃者は PLC システムへのラテラルムーブメントを実行した。

ネットワークスキャンの過程で、Windows OS 基盤の PLC (Programmable Logic Controller) システムが攻撃者にさらされた。PLC システムはシステム名を製品名で設定していたため、攻撃者がシステムを特定できた。また、メーカーの初期パスワードを使用しており、ログオン攻撃に脆弱な状態であった。同じメーカーの同じ製品が複数存在し、同じパスワードで管理されていたために侵害規模が拡大した。

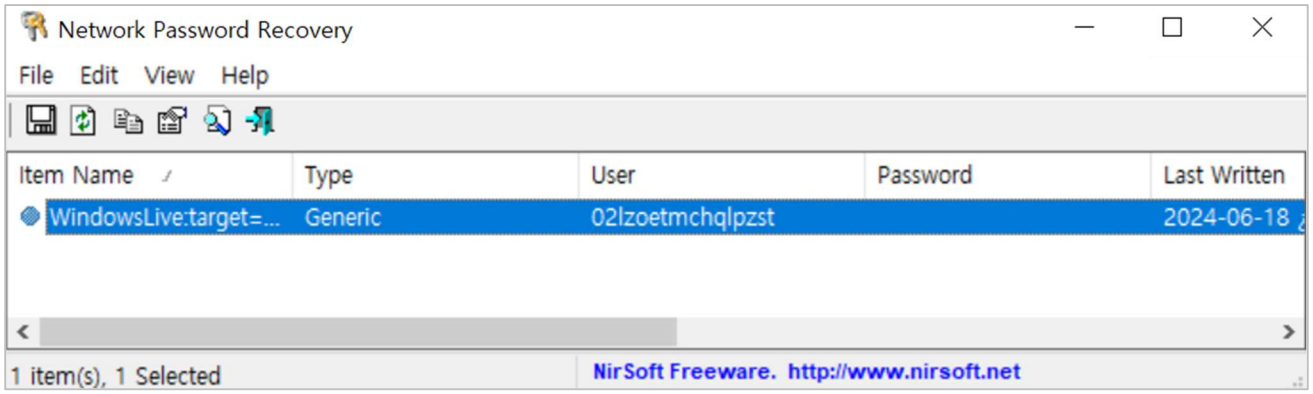


図5. netpass のイメージ

この過程では、管理者アカウントのログオンスキャン攻撃の痕跡は確認されていない。攻撃者が、被害システムのアカウント情報を知っていたと思われる。アカウント情報を収集した経路は確認されていないが、攻撃者が外部からアカウント情報を収集した、またはラテラルムーブメントのための情報収集段階で PLC システムのアカウント情報を収集していたと思われる。

検知の回避

PLC システムには別途アンチウイルスプログラムがインストールされていなかったが、Windows Defender が動作していた。攻撃者は Windows Defender の無効化ツールを利用して、アンチウイルスプログラムによる不正なランサムウェアファイルの検知を回避した。

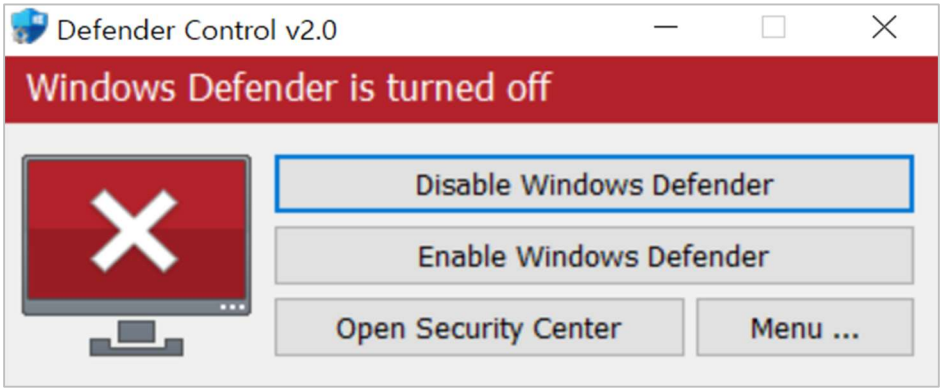


図6. Windows Defender の無効化

ランサムウェア感染

Windows Defender を無効にした攻撃者は、運用 PC および PLC システムに対しランサムウェアを配布した。被害システムにおいて確認されたランサムノートは Phobos 系列のランサムウェアのランサムノートと同じであり、ランサムウェアに感染したファイル拡張子の形式も Phobos 系列のランサムウェアと同様で、Phobos 系列のランサムウェアに感染したと確認された。

encrypted

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail
Decipher@mailfence.com
Write this ID in the title of your message [redacted]-3510
Or write us to the TOX messenger:
527185CB5EAB7CD8E52D2A52ADA93040BFFB5894331665EAA14A0D4AE83C1176059BAF07E91A
You can download TOX messenger here https://tox.chat/
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the tool that will decrypt all your files.

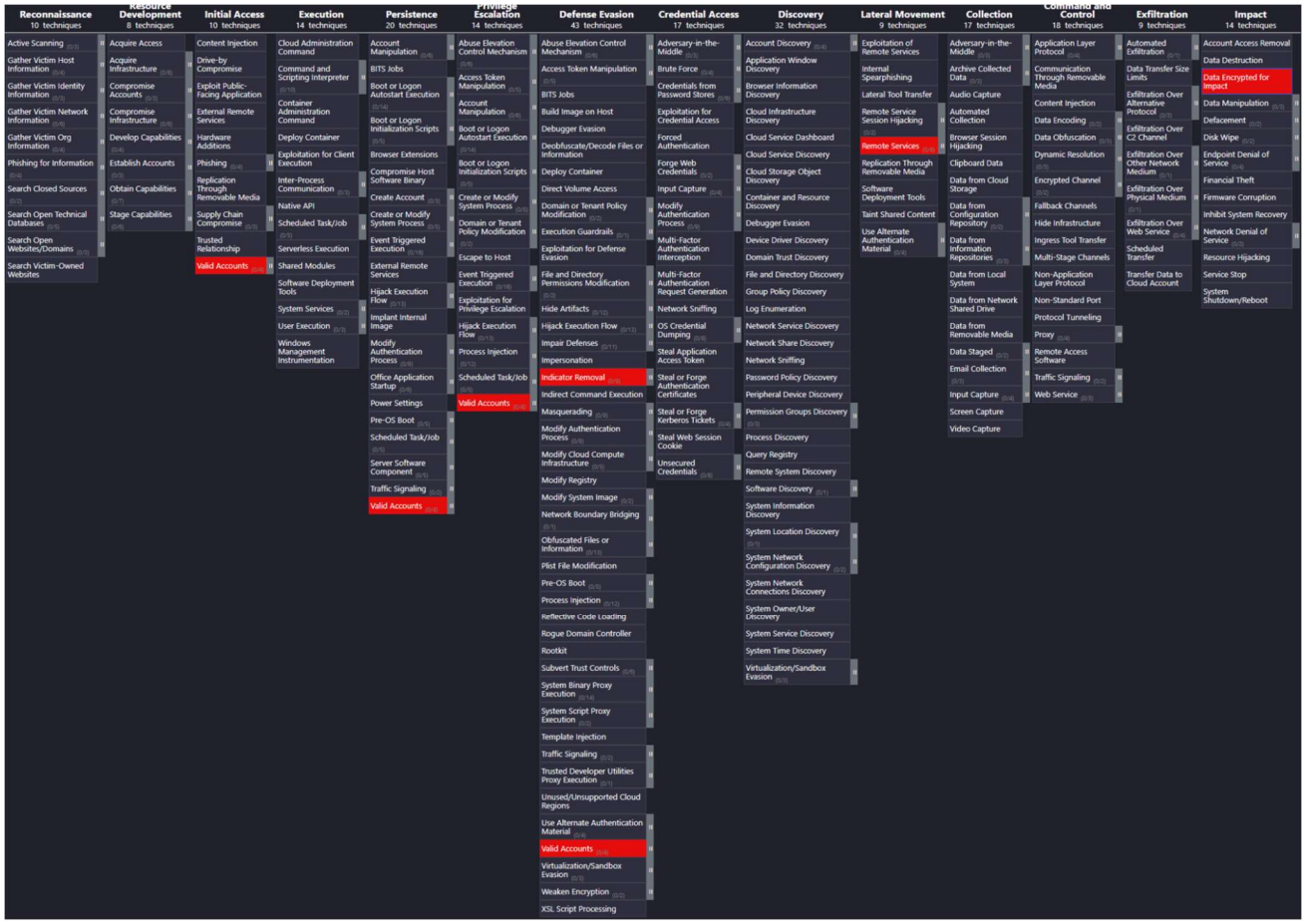
Free decryption as guarantee
Before paying you can send us up to 3 files for free decryption. The total size of files must be less than 4Mb (non archived), only text document or image

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

図7. Phobos 系列のランサムウェアのランサムノート

MITRE ATT&CK



Tactics	TID	使用された技術
Reconnaissance		
Resource Development		
Initial Access	T1078.003 Valid Accounts: Local Accounts (外部サイト、英語にて提供)	Administrator アカウントの使用
Execution		
Persistence	T1078.003 Valid Accounts:	Administrator アカウントの使用

	Local Accounts (外部サイト、英語にて提供)	
Privilege Escalation	T1078.003 Valid Accounts: Local Accounts (外部サイト、英語にて提供)	Administrator アカウントの使用
Defense Evasion	T1070.004 Indicator Removal: File Deletion (外部サイト、英語にて提供)	使用した不正ファイルの削除
	T1078.003 Valid Accounts: Local Accounts (外部サイト、英語にて提供)	Administrator アカウントの使用
Credential Access		
Discovery		
Lateral Movement	T1021.002 Remote Services: SMB/Windows Admin Shares (外部サイト、英語にて提供)	ネットワークログオン (Administrator)
	T1021.001 Remote Services: Remote Desktop Protocol (外部サイト、英語にて提供)	リモートデスクトップログオン (Administrator)
Collection		
Command and Control		
Exfiltration		
Impact	T1486 Data Encrypted for Impact (外部サイト、英語にて提供)	ランサムウェア感染

Threat Hunting Rules

Rule	Query
1	**SELECT** * **FROM** Registry_Event **WHERE** registry.Path = '(HKLM|HKCU)¥Software¥Microsoft¥Windows¥CuttentVersion¥Run' **AND** registry.Keyname = 'AntiRecuvaDB'
2	**SELECT** * **FROM** File_Event **WHERE** File.FileName **LIKE** '%.%.id[%.%].[%@%.com].[%]' **AND** File.FileName = 'info.hta'
3	**SELECT** * **FROM** Registry_Event **WHERE** registry.Path = '¥Software¥Policies¥Microsoft¥Windows Defender' **AND** registry.Keyname = 'DisableAntiSpyware' **AND** registry.Value <> '0'
4	**SELECT** * **FROM** Registry_Event **WHERE** registry.Path = 'HKLM¥Software¥Wow6432Node¥Policies¥Microsoft¥Windows Defender¥' **AND** registry.Keyname = 'DisableAntiSpyware' **AND** registry.Value <> '0'

IoC (Indicators of Compromise)

不正ファイル

No	MD5 Hash	File Name	アンラボの検知名
1	f627c30429d967082cdcf634aa735410	netpass64.exe	HackTool/Win.PSWTool.R345815(2022.09.02.00)
2	bd7756138f48dc4ec8088e23ef6a4c80	AntiRecuvaDB.exe	Ransomware/Win.Phobos.R363595(2023.08.24.00)
3	10d8e4ca3fa2902859c77f41baee4dda	dfControl.exe	HackTool/Win.DefenderControl.R443408(2021.10.07.03)

More security, More freedom

株式会社アンラボ

〒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)

| https://www.ahnlab.com/jp

このレポートは著作権法により保護されており、営利目的の無断転載と無断複製を禁止します。

このレポートの内容のすべてまたは一部引用、加工時、アンラボから発行されたことを明記してください。

＊ このレポートに収録された内容の配布についてのすべての問い合わせは

AhnLab までお願いいたします。

このレポートは https://atip.ahnlab.com を通して利用できます。

© 2024 AhnLab, Inc. All rights reserved.

AhnLab