アンラボ・セキュリティレター

Press Ahn

2021.1　Vol.85

流通大手企業 A 社を攻撃した CLOP ランサムウェアの解析レポート公開

AhnLab、CLOPランサムウェアを深層解剖

流通大手企業 A 社を攻撃した CLOP ランサムウェアの解析レポート公開

昨年11月、セキュリティ業界だけでなく、韓国国内産業群の全体を騒がせた事件が発生した。屈指の流通大手である E-Land システムが「CLOPランサムウェア」(CLOP Ransomware)に感染したのである。A社関係者の言葉を引用した報道によると、全体オフライン店舗のうち約半分が影響を受け、営業に支障を来たしたと発表された。この事件は、ランサムウェアが企業の規模を問わないという事と、さらに、このような攻撃が韓国国内産業において現実味をおびてきたという事実を実感させるきっかけとなった。

今回 AhnLab は、E-Land を攻撃した CLOP ランサムウェアの拡散経路および復旧の可能性、そして CLOP ランサムウェアの攻撃プロセスと変化の動向を綿密に分析したレポートを公表した。この記事では、当該レポートにおいて取り上げた内容を簡略に考察していく。

まず、E-Land への攻撃事例を扱う前に、CLOP ランサムウェアに対する解析を行う必要がある。CLOP ランサムウェアの攻撃プロセスおよび変化の推移について把握することが、より実際の事例を明確に理解できるためである。

CLOP ランサムウェアの攻撃対象とプロセス

攻撃対象

CLOP ランサムウェアは、Active Directory(AD)を運用している企業を攻撃対象とした。AD は一元化した管理を通して多数の Windows システムを効率的に管理できるため、個人のユーザーよりも主に企業で使用されている。攻撃者は、この点を悪用して AD サーバーの管理者権限を奪取し、企業内の多数のシステムを攻撃した。

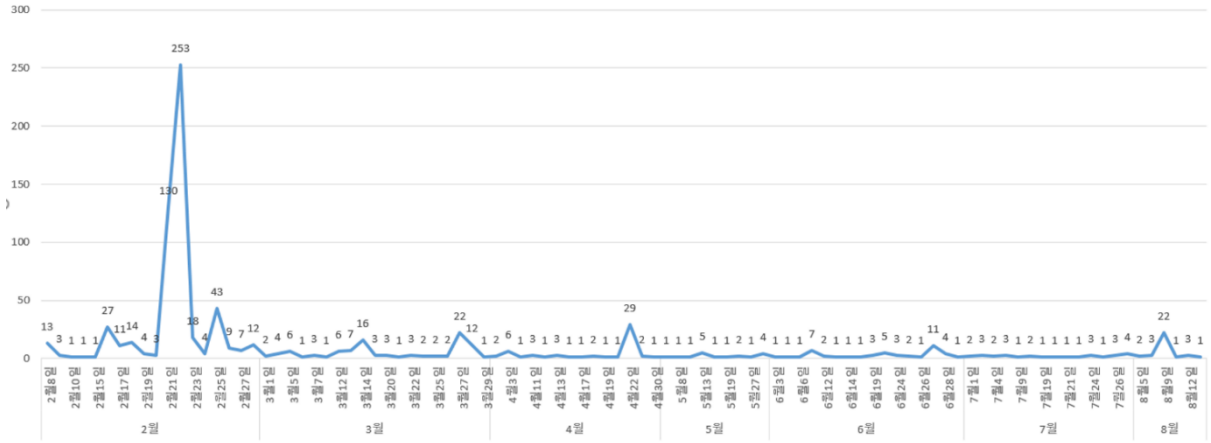
AhnLab は2019年に発生したランサムウェアにより被害を受けた企業は369社、システム(PCおよびサーバー)は13,497個と把握している。ただし、集計された数字は企業を対象とした攻撃のみであるため、把握されていない被害システムまで含めると、これよりもはるかに多いものと予想される。

攻撃対象は、公共機関、教育、放送、金融/証券/保険、製造業、IT、流通、通信事業者など幅広く、特定業界に限定されていない。2019年上半期基準、割合で見るとランサムウェア被害のほとんどが製造業(53%)で発生しており、金融(15%)、情報サービス(11%)、卸小売(9%)分野がそれに続いていた。

攻撃者は、企業をターゲットにするために精巧に製作したスピアフィッシング(ターゲットを特定して攻撃を行うこと)攻撃を利用している。電子メールの受信者を明確に指定して攻撃を試み、本文の内容は攻撃対象の使用言語に合わせて精巧に作成されている。ひとつ注目すべき部分は、攻撃者がロシア以外の国を攻撃対象としていることである。キーボードレイアウトと文字セットを確認し、ロシアや独立国家共同体(CIS)である場合、CLOP ランサムウェアが動作しないようにしていた。

ランサムウェアの変種

以下は、2019年上半期に発見された CLOP ランサムウェアの変種数の変化である。2019年2月に CLOP ランサムウェアの変種が複数発見された。参考に、CLOP ランサムウェアのランサムノート「ClopReadMe.txt」がインターネット上の Pastebin.com に初めて公開された時点は2019年2月8日である。



[図1] 2019年における CLOP ランサムウェアの変種変化

攻撃プロセス

攻撃は大きく分けて準備、掌握、実行段階に分かれている。細分化すると、10段階まで存在し、CLOP ランサムウェアの実際の配布と実行は、攻撃の最終段階である。細分化した10段階を要約すると、以下の通りである。

準備	**最初の攻撃対象に電子メールで不正な文書ファイルを添付して送信し、遠隔操作マルウェアをインストール**
1	電子メールに添付された不正な文書ファイル(Excel、Word)をユーザーが閲覧
2	文書ファイルに挿入されたマクロにより、遠隔操作マルウェアのダウンローダー実行
3	当該システムが AD(Active Directory) を導入/運用している場合、 遠隔操作マルウェアのファイルをダウンロードして実行(AD 環境を狙う)
4	遠隔操作マルウェアのファイルは、当該システムにCobalt Strikeビーコンをインストール
掌握	**Cobalt Strikeを利用してAD内のシステムを掌握**
5	ADドメインの構成情報を確認
6	脆弱性を利用して実行権限を昇格
7	昇格した権限によりMimikatzモジュールを実行、ローカル管理者アカウントまたは ADドメイン管理者アカウントのクレデンシャルを獲得
8	ADドメイン管理者アカウントの獲得に成功すると、 ドメインコントローラサーバーに接続してドメインに連結されたシステムを掌握
実行	**AD内のシステムを対象にCLOPランサムウェアへの感染を実行**
9	ドメインコントローラの共有フォルダーにCLOPランサムウェア等のマルウェアを準備
10	ADドメインに連結されたシステムでタスクスケジュールまたはリモートコマンドを利用して、CLOPランサムウェアを配布および実行

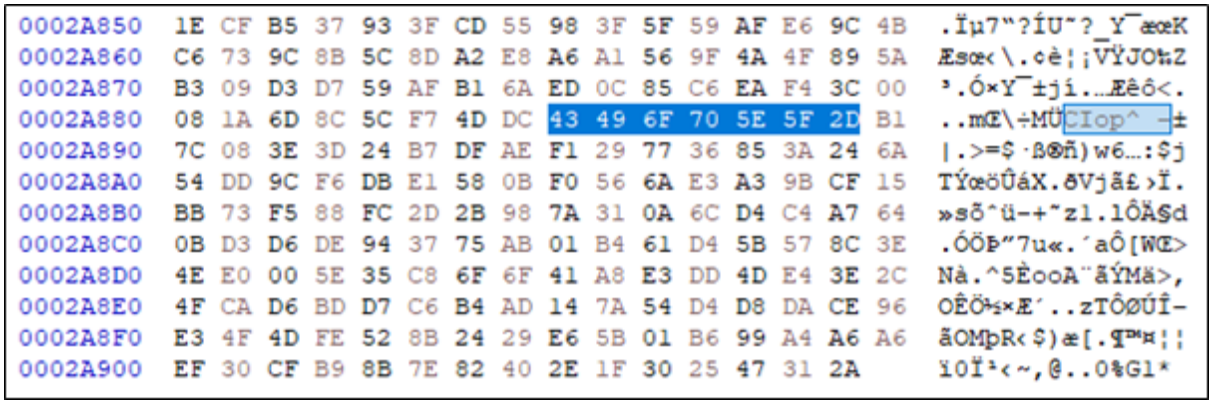
[表1] CLOP ランサムウェアの攻撃プロセス

CLOP ランサムウェアの変化の推移

過去と比較すると、CLOP ランサムウェアは暗号化方式とサービス型動作など、本質的には大きく変わっていない。違いがあるとすれば、プロセス終了ルーティンおよび暗号化除外パスで文字列の代わりに CRC を求めてから比較する方式に変更された点が挙げられる。

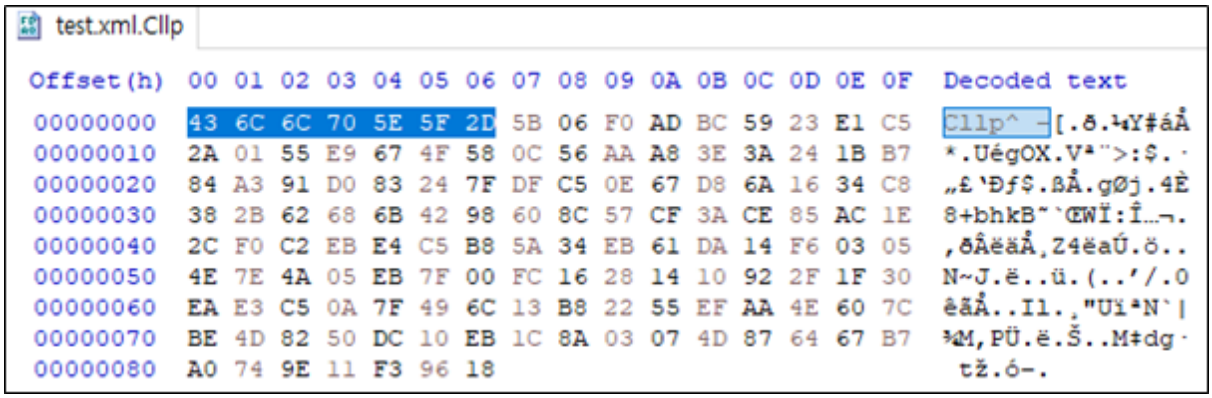
最近の CLOP ランサムウェアの変化

ただし、2020年下半期に収集された CLOP ランサムウェアではさらなる変化が確認された。過去バージョンの場合、暗号化されたファイルの公開にシグネチャと一緒に公開鍵で暗号化された対称鍵が付け加えられた形式だったが、最近確認された CLOP ランサムウェアは同じ名前に「.Clp」という拡張子を付けて新しく生成したファイルに、シグネチャと暗号化された鍵を保存している。



0002A850	1E	CF	B5	37	93	3F	CD	55	98	3F	5F	59	AF	E6	9C	4B
0002A860	C6	73	9C	8B	5C	8D	A2	E8	A6	A1	56	9F	4A	4F	89	5A
0002A870	B3	09	D3	D7	59	AF	B1	6A	ED	0C	85	C6	EA	F4	3C	00
0002A880	08	1A	6D	8C	5C	F7	4D	DC	43	49	6F	70	5E	5F	2D	B1
0002A890	7C	08	3E	3D	24	B7	DF	AE	F1	29	77	36	85	3A	24	6A
0002A8A0	54	DD	9C	F6	DB	E1	58	0B	F0	56	6A	E3	A3	9B	CF	15
0002A8B0	BB	73	F5	88	FC	2D	2B	98	7A	31	0A	6C	D4	C4	A7	64
0002A8C0	0B	D3	D6	DE	94	37	75	AB	01	B4	61	D4	5B	57	8C	3E
0002A8D0	4E	E0	00	5E	35	C8	6F	6F	41	A8	E3	DD	4D	E4	3E	2C
0002A8E0	4F	CA	D6	BD	D7	C6	B4	AD	14	7A	54	D4	D8	DA	CE	96
0002A8F0	E3	4F	4D	FE	52	8B	24	29	E6	5B	01	B6	99	A4	A6	A6
0002A900	EF	30	CF	B9	8B	7E	82	40	2E	1F	30	25	47	31	2A	

[図2] 過去の CLOP ランサムウェア - 暗号化されたファイルの後部に追加された対称鍵



test.xml.Cllp

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	43	6C	6C	70	5E	5F	2D	5B	06	F0	AD	BC	59	23	E1	C5	Cllp^ -[.ð.¼Y#áÅ
00000010	2A	01	55	E9	67	4F	58	0C	56	AA	A8	3E	3A	24	1B	B7	*.UégOX.Vª¨>:$.·
00000020	84	A3	91	D0	83	24	7F	DF	C5	0E	67	D8	6A	16	34	C8	„£'Ðƒ$.ßÅ.gØj.4È
00000030	38	2B	62	68	6B	42	98	60	8C	57	CF	3A	CE	85	AC	1E	8+bhkB˜`ŒWÏ:Î…¬.
00000040	2C	F0	C2	EB	E4	C5	B8	5A	34	EB	61	DA	14	F6	03	05	,ðÂëäÅ¸Z4ëaÚ.ö..
00000050	4E	7E	4A	05	EB	7F	00	FC	16	28	14	10	92	2F	1F	30	N~J.ë..ü.(..'/.0
00000060	EA	E3	C5	0A	7F	49	6C	13	B8	22	55	EF	AA	4E	60	7C	êãÅ..Il.¸"UïªN`|
00000070	BE	4D	82	50	DC	10	EB	1C	8A	03	07	4D	87	64	67	B7	¾M‚PÜ.ë.Š..M‡dg·
00000080	A0	74	9E	11	F3	96	18										tž.ó-.

[図3] 最近発見された CLOP ランサムウェア - .Clp ファイルに対称鍵を保存

また、他のプロセスを終了させるルーティンと、ボリュームシャドウコピーを削除するルーティンがなくなっている。しかし、プロセスを終了させるルーティンを実行する同じ証明書を持つファイルが同時に確認されており、CLOP ランサムウェアのバイナリ自体ではなく、追加ファイルでこれらの機能を担当する形式に変更されたということが推定できる。

```
ShellExecuteA(0, 0, "cmd", "/C net stop McAfeeEngineService /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C taskkill /IM dbsnmp.exe /F", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop \"Symantec System Recovery\" /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop NetMsmqActivator /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C taskkill /IM steam.exe /F", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop MSExchangeMGMT /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop SepMasterService /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C taskkill /IM PNTMon.exe /F", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop tmlisten /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop BackupExecDeviceMediaService /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop ShMonitor /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C taskkill /IM dbeng50.exe /F", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop VeeamRESTSvc /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop BackupExecVSSProvider /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop MsDtsServer /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop VeeamDeploySvc /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C taskkill /IM powerpnt.exe /F", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop SQLAgent$PROD /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop \"Sophos Message Router\" /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop McShield /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop BackupExecJobEngine /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop swi_filter /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop \"Sophos AutoUpdate Service\" /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop \"Sophos MCS Agent\" /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop MsDtsServer100 /y", 0, 0);
```

[図4] プロセス終了機能を持つファイルの発見

パッキング方式も変更された項目のうちの一つである。CLOP ランサムウェアは FlawedAmmyy など、他のマルウェアと同じパッカーのアウトラインを有している。すなわち、ファイル診断を回避するためにオリジナルのバイナリをエンコードして持っており、パッカーが実行されるとメモリ上でデコードされたオリジナルのバイナリを実行する。

ランサムノートの変化

2019年には、CLOP ランサムウェアのランサムノートファイルの内容に大きな変化はなかった。ランサムノートは、ファイルが暗号化されたことを知らせる目的と、注意事項および攻撃者の電子メールアドレスが主な内容である。しかし、2020年10月頃から確認された CLOP ランサムウェアは、暗号化されたファイルを復旧するための連絡先以外にも、企業の機密データをディープ Web (Deep Web) に公開するという内容を記載し始めた。参考に、以下の企業(SOFTWARE AG)は、ランサムノートに記載されたディープ Webサイトに CLOP ランサムウェアによって流出された情報が公開された。

HELLO DEAR SOFTWARE AG

YOUR NETWORK IS ENCRYPTED!

ALL YOUR FILES ARE ENCRYPTED!

Also a lot of sensitive data has been downloaded from your network.

For example:

¥¥10.137.1.81¥Finance¥Private

¥¥10.137.1.81¥Finance¥Share

¥¥10.66.20.19¥Finance

¥¥10.66.20.19¥Contracts

¥¥10.21.32.57¥MandAProjects

This is a small part, about 10%.

If you refuse to cooperate, all data will be published for free download on our portal:

http://ekbgzchl6x2ias37.onion/ (use TOR browser)

mirror http://ekbgzchl6x2ias37.onion.dog/

To get access to your files back, contact us by email:

unlock@goldenbay.su

or

unlock@graylegion.su

AND

dromotelllinghoettd@tutanota.com

or write to the chat at:

http://geqwmtbpciqqhs7nsw5crgwtqw7mncatrz65bkrpcfpwtv424uszsbid.onion/?u=FR1GMMX2WCE4XI3Z3H38Q7CG628J7OOS5VEX71594937HCWQJ5OFI7LFFZ4SDIAO (use TOR browser)

!!! DO NOT ATTEMPT TO RESTORE OR MOVE THE FILES YOURSELF. THIS MAY DESTROY THEM !!!

CI0p-_^

[図5] 情報流出の脅迫内容が含まれたランサムノート

流通大手企業、E-Landへの攻撃分析

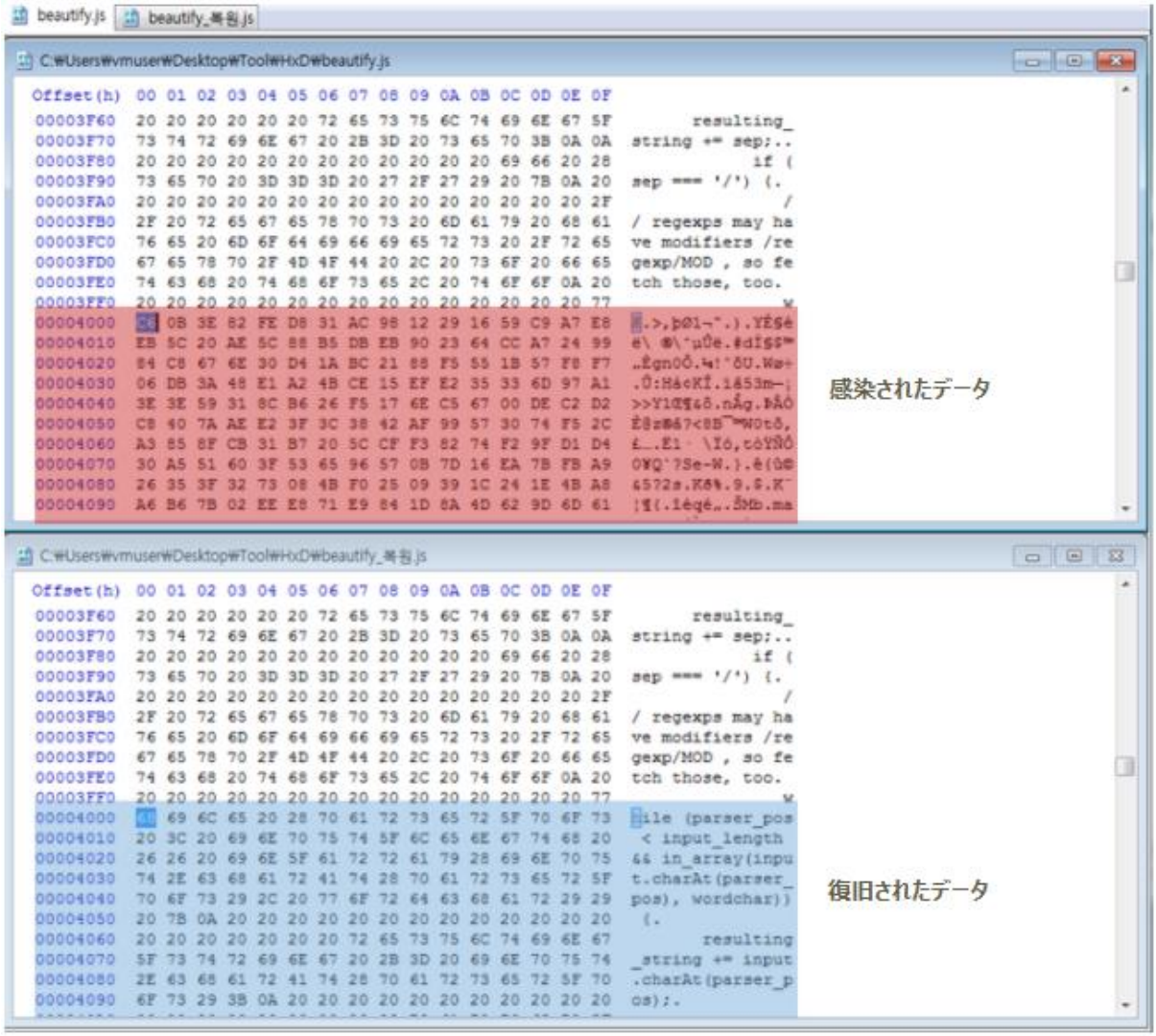
ここで、これまで説明してきた CLOP ランサムウェアの攻撃に関する分析情報をもとに、E-Land に対して実行された攻撃について簡単に分析していく。

まず、従来の CLOP ランサムウェアのように、A社への攻撃に使用された CLOP ランサムウェアに感染したシステムは、復旧が不可能である。このランサムウェアは、対称鍵アルゴリズムを利用して各ファイルを暗号化したあと、バイナリ内部に存在する公開鍵で対称鍵を暗号化している。つまり、その公開鍵に対応する秘密鍵を知らなければ、暗号化されたファイルを復旧することは不可能である。

ただし、暗号化された鍵を保存する方法に違いがある。前半で CLOP ランサムウェアの変化の推移から分析したように、初期バー

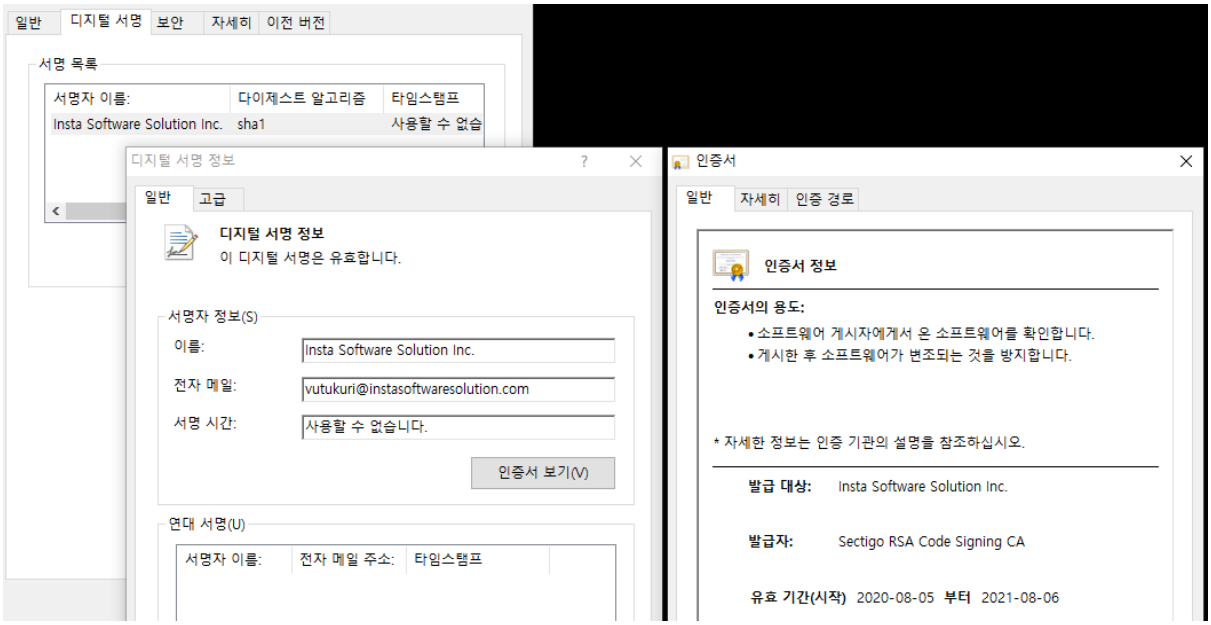
ジョンでは暗号化されたファイルの後部に特定のシグネチャと同時に暗号化された鍵が付け加えられた構造であった。しかし、最近確認された CLOP ランサムウェアは暗号化されたファイルと同じファイル名(正常なファイル名を維持)の後部に「.Cllp」拡張子を付けた追加ファイルを生成し、その .Cllp ファイルに関連する鍵を保存している。E-Land への攻撃に利用された CLOP ランサムウェアも、後者に該当する。

攻撃者が持つ秘密鍵が不明なためファイルの復旧が不可能だが、以前とは異なりボリュームシャドウコピー(Windows の標準機能で、特定の時刻のファイル、フォルダーまたはボリュームのコピーを保存しておいたもの)を削除するコマンドが存在しない。したがって、システムにランサムウェア感染前の復元ポイントが存在すれば、Windows の復元機能を利用して感染前の状態に戻すことができる。



[図6] 感染したファイルと復旧されたファイル

また、E-Land への攻撃に使用された CLOP ランサムウェアのファイルは、以下の通り有効なデジタル署名の証明書情報を含んでいる。



[図7] E-Landを攻撃した CLOP ランサムウェアに使用された証明書

AhnLab は、E-Land を攻撃した CLOP ランサムウェアと同じ証明書を持つファイルを多数確認した。分析結果によると、この証明書を有する別のファイルは10月から出回っており、ランサムウェアだけでなく Windows Defender のアンチウイルスプログラムを無力化するためのファイルとしても製作されている。すなわち、同じグループが同じ証明書で CLOP ランサムウェア以外にも様々なマルウェアを製作しているという事が推測できる。

結論として、攻撃者は精巧で緻密な戦略により企業を攻撃したということである。AD によって複数のシステムを制御できるという点を悪用し、CLOP ランサムウェアのマルウェアを配布した。このプロセスで、攻撃者は悪意ある操作のマルウェアをインストールしてシステム管理者権限を取得する。CLOP ランサムウェアによる被害だけでなく、内部情報の流出および管理者アカウントが奪取されるため、企業は莫大な被害を受けることになる。攻撃者は、ファイルの暗号化とランサムウェアに感染された事実、窃取した内部の情報を外部への公開などで企業を脅迫してお金を要求する。ファイルの暗号化と内部情報流出という二つの質によって攻撃対象を脅迫する最近の傾向に、CLOP ランサムウェアの攻撃者も従っている。

2019年から発生している CLOP ランサムウェアによる攻撃は、2020年現在も続いている。攻撃者は、マルウェアの拡散と攻撃の手法を変化させつつ、進化を続けている。特に、企業の AD サーバーを掌握してもすぐにランサムウェアを実行せず、潜伏待機するケースも発見されている。ランサムウェアによる攻撃が発生しても、これをトレースバック解析することも時間的上困難になっている。

攻撃に備えるためには、個人と企業の両方が努力する必要がある。何よりも、個人のセキュリティ意識向上が重要である。十分なユーザー教育を通してスピアフィッシングの被害に遭わないようにしなければならない。そして、ソフトウェアを最新バージョンにア

ップデートすること、セキュリティプログラムの動作有無を確認することである。また、重要なドキュメントやファイルはバックアップしておき、トラブルに備えなければならない。企業の場合、AD のセキュリティには特に注意を払い、アカウント情報の管理を徹底しなければならない。セキュリティソフトウェアを導入した場合は、定期的なモニタリングを通してシステムの異常兆候をすぐに把握することが重要である。

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)