NOZOMI NETWORKS

新種ランサムウェア“LockerGoga”とは

～ランサムウェア攻撃で操業停止に追込まれた Norsk Hydro 社～

TRILOGY
In collaboration with customer

株式会社テリロジー

はじめに

2010年にイランにあるウラン濃縮工場の遠心分離器を破壊した“Stuxnet”の登場以降、海外ではエネルギープラントや産業制御システムなど重要インフラへのサイバー攻撃が増加している。
2014年には、ドイツの鉄鋼工場で起こったサイバー攻撃、2016年12月にウクライナの首都キエフで送電網を狙った“Industroyer”、そして2017年に中東の石油化学施設へのサイバー攻撃で莫大の被害を与えた凶悪なマルウェア“TRITON”。そして2019年3月にノルウェーの世界最大級のアルミ製造工場を狙ったランサムウェア“LockerGoga”。続々と新種の凶悪なサイバー攻撃が世界各地の重要インフラを狙っている。早急なるセキュリティ対策が叫ばれている。今回は今年3月に起きた“LockerGoga”について俯瞰する。


（Norsk Hydro社提供）

アルミニウム製造と再生エネルギーの世界最大級のメーカ、Norsk Hydro 社（世界 40 か国、従業員 3.5 万人以上）がランサムウェア“LockerGoga”攻撃によって大きな打撃を受けた。
ノルウェーのオスロを本社拠点とする同社は、この攻撃によってアルミニュウム製造工場の従業員達は手動操作への切り替え製造を余儀なくさせられたと発表した。
Norsk Hydro 社は現在、この攻撃を封じ込め、無効化するための努力をしている。**“**現時点ではまだ、全体の被害範囲と損害総額についてはつかんでいない**”**と同社は Facebook で声明を出した。

“どの製造設備システム（産業制御システムも含む）も外部ネットワークには接続していない”と同社は語っている。Norsk Hydro 社の Web サイトもこの声明を発表した時点では停止していた。

同社は毎年 50 万トン近くのアルミニウム製品を製造しており、また北欧諸国に電力を供給する重要な水力発電での電力供給事業者でもある。

ロイター通信は、カタールとブラジルでの操業も手動に切り替えたと報道したが、同社はノルウェー以外の主要工場への影響はないとノルウェー証券取引所に報告している。

同社の広報担当者は“Norsk Hydro 社全体への影響状況と顧客への影響を今判断するのは時期尚だ”と語った。

ノルウェーの国家安全保障局(NSA)は今回のインシデントに対してコメントはしなかったが、このインシデントが今まで検出されなかった新種のランサムウェア“LockerGoga”である可能性が高いとロイターに語った。ランサムウェアはユーザファイルをロックし、ロック解除用の復号化キーを条件に身代金支払いを要求する手口の悪質なマルウエアとして知られている。

セキュリティ専門家 Kevin Beaumont 氏（SoC manager,BNFL,UK）は、今月初めフランスのパリを拠点とするコンサルティング会社 Altran Technologies をサイバー標的とするためにこのマルウェアが使用されたと語った。Kevin Beaumont 氏はこのマルウェアは他のランサムウェアのように外部の悪意なコマンド＆コントロールサーバ(C&C)への接続を必要としないとコメント。マルウェア分析サイト VirusTotal では、まだ LockerGoga マルウェアの対応ツールはほんの一握りのベンダーであると語っている。

現在、Norsk Hydro 社は手動モードに切り替えるか、またはサイバー攻撃を受けた工場でのアルミニウム製造を一時的に停止するかを検討している。ノルウェーの国家安全保障局(NSA)とノルウェーの地元メディアは、このインシデントを“**LockerGoga**”と呼ばれるランサムウェア攻撃として断定した。この攻撃は明らかに同社製造システムを標的にした。

このサイバー攻撃の重大性を判断して、Nozomi Networks Labs は翌日の 3 月 19 日（現地時間）に　LockerGoga の調査分析を開始した。

Norsk Hydro 社は、世界最大級のアルミニウム生産企業。いくつかの施設がランサムウェア攻撃の影響を受けており、機能停止や手動制御システムへの切り替えを余儀なくされた。この写真は Norsk Hydro 社による画像提供である。

ランサムウェア攻撃がアルミ製造工場に致命的な打撃を与えた

報道メディアによると、マルウェア攻撃はオスロ時間（UTC + 1）の 3 月 18 日月曜日の夕方に始まった。3 月 19 日、同社の Web サイトは不能になり、製造工場への影響が報告された:

- 融解アルミニウム状況を監視し、1 日 24 時間稼働し続ける必要がある主要ラインは手動操作モードに切り替えられた
- いくつかの工場は製造停止を余儀なくされた
- いくつかの金属押出加工工場が閉鎖された
- 水力発電所は正常に機能している

LockerGoga ランサムウエアとは？

Nozomi Networks Labs は SHA256 のハッシュ関数の LockerGoga サンプルをベースに緊急分析を行った:

`6e69548b1ae61d951452b65db15716a5ee2f9373be05011e897c61118c239a77`

ランサムウェアは下記の特定拡張子を持つファイルを暗号化することが出来る:

`doc, dot, wbk, docx, dotx, docb, xlm, xlsx, xltx, xlsb, xlw, ppt, pot, pps, pptx, potx, ppsx, sldx, pdf`

攻撃者の主な目的は、上記の拡張子を含むファイルのユーザにとって重要なデータファイルを暗号化すること。実際には、暗号化フレーズの最後に、README-NOW.txt というメッセージが組み込まれる（以下参照）。そして、READ.ME ファイルに身代金要求を提示する。尚、この脅迫メッセージでは、ユーザはファイルを取り戻すために暗号通貨 Bitcoin を使って身代金を払うよう具体的な支払方法も示唆している。

Greetings!
There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.They would have damaged all of your data by mistake or for fun.Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.Without our special decoder it is impossible to restore the data.Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.will lead to irreversible destruction of your data.To confirm our honest intentions.Send us 2-3 different random files and you will get them decrypted.It can be from different computers on your network to be sure that our decoder decrypts everything.Sample files we unlock for free (files should not be related to any kind of backups).We exclusively have decryption software for your situation.
DO NOT RESET OR SHUTDOWN – files may be damaged.
DO NOT RENAME the encrypted files.DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.To get information on the price of the decoder contact us at:
AbbsChevis@protonmail.comIjuqodiSunovib98@o2.pl
The payment has to be made in Bitcoins.The final price depends on how fast you contact us.As soon as we receive the payment you will get the decryption tool and instructions on how to improve your systems security

LockerGoga はどのように振る舞うのか？

このマルウェアは、ファイルを暗号化してからファイルに身代金用メモを埋め込み、ファイルを取り戻すために必要な手順についてユーザに通知する。これは、殆どのランサムウェアマルウェアで使用されている古典的なアプローチである。
このマルウェアは他のファイルに拡散する機能はないが、セキュリティアナリストによると、このマルウエアはセキュリティ検知を回避するためにいくつかのアンチアナリシス技法を使用しているという。このマルウエアは仮想マシンの存在を識別したり、マルウエア

サンプルを収集されないようにするためにファイルシステムから自分自身を削除する機能を備えている。攻撃者はカスタム機能や複雑な機能（C&C、DNS ビーコンなど）をこのマルウェアコードに追加しなかったため、その目的はスパイ活動ではなく環境破壊であるという。一部の研究者達は、攻撃者はこのマルウェアを拡散させるためのメカニズムとして Active Directory を用いる可能性があると示唆している。想定されるシナリオ（NorCERT により確認済み）は以下の通り：

- 攻撃者は、標的企業の Domain Admin Group に登録されているシステムに侵入。
- 悪意のある実行可能ファイルを Netlogon ディレクトリに配置して、すべてのドメインコントローラに自動的に伝播するようにする。
- ファイアウォールの多くはデフォルトで Active Directory 情報を許可しているのでこれを利用する。

LockerGoga に感染しているかをどうやって知るのか？ どのようにしてそれを取り除くのか？

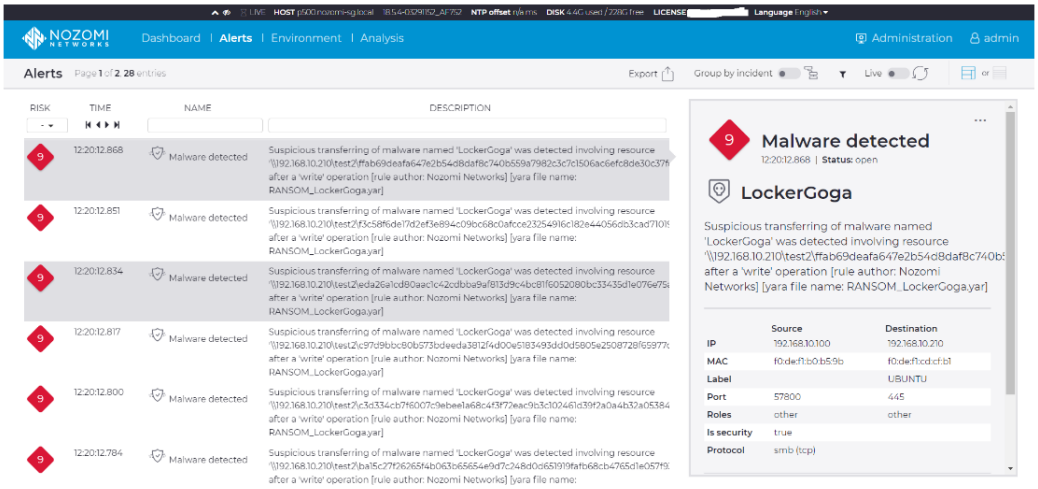
標的のファイルは暗号化され、ファイル拡張子の末尾に“.locked”というファイル拡張子が追加されるので感染されたかどうかは特定出来る。
MS-ISAC では、「ランサムウェアに対して最も重要な対策は、バックアップから復旧できる態勢の確立」だと指摘し、バックアップから確実に復旧できるよう普段からテストを実施しておくよう呼び掛けている。これが現在のところの唯一の方法である。
Nozomi Networks の OT ThreatFeed(OTTF)のアップデート（以下画面参照）で、LockerGoga を検出する機能が含まれている（具体的には Yara ルールで定義）。

LockerGoga

```
// Created by Nozomi Networks Security Team

rule LockerGoga : ransomware lockergoga {
   meta:
      author = "Nozomi Networks"
      description = "LockerGoga Ransomware"
      name = "LockerGoga is a Trojan horse that encrypts files on the compromised computer and asks the user to pay in order to decrypt them."
      date = "20/03/2019"
      hash1 = "c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15"
      hash2 = "6e69548b1ae61d951452b65db15716a5ee2f9373be05011e897c61118c239a77"
      hash3 = "bdf361278174l3f625d2625d3133760af724d6ad2410bea7297ddc116abc268f"
      hash4 = "47f5a231f7cd0e36508ca6ff8c21c08a7248f0f2bd79c1e772b73443597b09b4"

   strings:
      $s0 = "licensed by Dinkumware, Ltd. ALL RIGHTS RESERVED" wide ascii
      $s1 = "$error_info_injector@"
      $s2 = "Sectigo Limited"
      $s3 = "\\crypto-locker\\"
      $s4 = "wIBEQ=="
      $s5 = "You should be thankful that the flaw was exploited" wide ascii
      $s6 = "Your files are encrypted with the strongest military" wide ascii
      $s7 = ".locked"
      $s8 = ".rdata$zzzdbg"
      $s9 = "\\([xX]86\\)" wide
      $10 = "|[A-Za-z]:\\cl.log" wide

   condition:
      uint16(0) == 0x5a4d and (filesize > 800KB and filesize < 1300KB) and ( 5 of them )
}
```

Nozomi Networks **OT ThreatFeed** は、LockerGoga の Yara Rule に更新された。

LockerGoga の検体サンプルを入手し、テリロジー社内疑似ネットワークに流して Nozomi Networks の SCADAguardian システムで検知した事を確認した。その画面を以下に示す。



Norsk Hydro 社はインシデントレスポンスの一環として革新的なコミュニケーションアウトリーチ手法を活用

長期間にわたってサイバー攻撃を受けたことを明らかにしない多くの企業とは異なり、Norsk Hydro はまったく異なるアプローチを取っている。彼らは攻撃に関するライブストリームのブリーフィングを直ぐに作成し、Facebook チャンネルで定期的に最新情報を提供している。

（注）アウトリーチとは、英語で「手を伸ばす」という意味で、この手法を用いて研究者や研究機関がその成果を広く国民に公開し還元するコミュニケーションを云う。

重要インフラへの LockerGoga 攻撃は対岸の火事ではない

Norsk Hydro への LokerGoga 攻撃は、産業分野を襲った最新のサイバー攻撃であり、大きな被害をもたらす可能性がある。以下に過去のサイバー攻撃例を参照する:

- 2012 年には、マルウェアによる攻撃で被害を受けたサウジアラムコ（サウジアラビア国有石油会社）の復旧に約 10 億ドルの費用がかかり、35,000 台の損傷したコンピュータを交換した。
- 米国ホワイトハウスによると、2017 年の NotPetya 攻撃により、世界中のサプライチェーン企業が 100 億ドルの損害を被ったという。 例えば、米国大手製薬会社 Merck（メルク）の損害額は 8 億 7000 万ドルだった。

今後、重要インフラの LockerGoga の影響を最小限に抑えるために、以下の対策が提案される：

- フィッシングメールの疑いのあるメールを受信した場合の対応策を社員に徹底する
- **重要インフラシステムの最新のバックアップを取っているかを確認する**
- **マルウェアの追跡および異常なビヘイビア（挙動）を迅速に特定するソリューションを活用してシステムをモニタリングする。**

＜参考資料＞

Nozomi Networks の OT ThreatFeed™とは

OT ThreatFeed™は、Nozomi Networks によって検知、分析および調整された脅威アップデートをユーザに配信するオプションのサブスクリプションです。 これにより、新たな脅威と脆弱性を迅速に検出し、IT / OT チームが最新の ICS リスクを常に把握出来るようにします。

Nozomi Networks の ICS セキュリティエキスパートチームは、複数のセキュリティ機関の情報源からの脅威と脆弱性情報を精査し、脅威の情報が正確で簡潔かつ実用的であることを確認します。 最新情報には、Nozomi Networks のセキュリティ研究チームが発見した脆弱性とマルウェアも含まれています。これは、ICS-CERT アドバイザリーに大きく貢献し、他の ICS コミュニティにも提供します。

タイムリーな脅威の更新

- 既知および新規の脅威と脆弱性のサイバー攻撃を特徴付ける指標を提供
- 複数の情報源からの ICS 脅威情報を精査し更新

―Nozomi Networks により発見された脅威のシグネチャ、追跡情報（IoC）およびゼロデイの更新

―ICS コミュニティの Yara ルールとパケットルールのアップデート

―米国政府の National Vulnerability Database（NVD）による脆弱性の更新

最後に

最近、LockerGoga だけでなく重要インフラを狙ったサイバー攻として Industoryer とか TRITON といった悪質なマルウエアの被害も増加傾向にある。我々国内でも、これらのインシデントを対岸の火事としてではなく、国内の重要インフラのこうした凶悪なランサムウエアへのサイバー攻撃対策が必要である。Nozomi Networks の研究チームは今後も引き続き LockerGoga に関するアップデート情報を提供予定。テリロジーも逐次これらのアップデート情報を Nozomi ユーザに提供する予定である。