サイバー攻撃の事例集

株式会社ICS研究所

自動車分野のセキュリティ事故事例

- 2005年米国で、外部から持ち込まれて接続されたノートPCにより、独ダイムラーの13の工場がWORM_ZOTOBなどの不正プログラムによって操業停止になった。
- 各工場の製造ラインが止まり、5万人の自動車工場の労働者は50分間作業ができない状態になり、1400万ドル（約17億円）の損害を出した。

■2008年に西日本の自動車会社の工場では、ベンダがエンジニアリング端末（操作パソコン）を入れ替えたところ、エンジニアリング端末にウィルスが混入していた。
■その結果、3日間程度工場の製造ラインの応答が遅くなり、原因究明には1ヶ月を要した

石油化学分野のセキュリティ事故事例

- 2008年トルコで、石油パイプラインが爆発した。パイプラインに設置されている監視カメラの通信ソフトの脆弱性を利用して内部ネットワークに侵入した。不正に動作制御系にアクセスし、管内の圧力を異常に高めて爆発を引き起こした。
- 攻撃者はすべての警報装置（カメラやセンサ）の動作を止め、通信を遮断するなどの操作も実施した。

Oil pipeline

Will Russell/CC BY 2.0　写真は参考画像です

Oil pipeline(全体図)

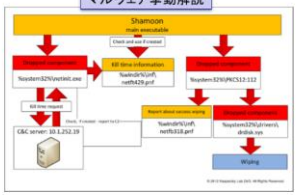
Source: Bloomberg research　　Bloomberg Graphics ®

化学分野のインシデント事例

●2012年、サウジアラビアの石油会社の制御システムで利用されるPC30,000台がマルウェアに感染。マルウェアの攻撃対象は、オイルの流れを止め、オイル製造事業の停止を狙っていた。
●攻撃により、内部ネットワークが1週間以上停止し、同ネットワークに接続されていたPCのディスクはすべて削除された。攻撃内容を調査したが、従業員が攻撃へ関与したか否か不明とのこと。

Oil Company

マルウェア挙動解説



出典：http://wired.jp/2012/08/28/worlds-largest-oil-producer-falls-victim-to-30k-workstation-attack/
http://securelist.com/blog/incidents/57784/shamoon-the-wiper-further-details-part-ii/

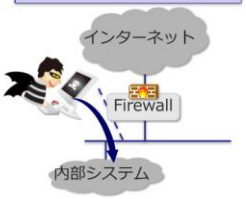
製鉄分野のインシデント事例

●2014年ドイツで、製鉄所の溶鉱炉のコントロールなど内部システムのコントロールを許可するユーザIDとパスワードが、攻撃者に電子メールに添付したマルウェアを使われ、不正入手されてしまう。
●溶鉱炉を正常に停止できず、生産設備が損傷する大きな被害を受けた。SCADAを攻撃対象として、SCADAの設定ファイルに悪意あるコードを追加した。

Steelworks

写真は参考資料（フェルクリゲン製鉄所-wikipedia）

攻撃者がリモートアクセス経路で内部システムに不正アクセス



出典：https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

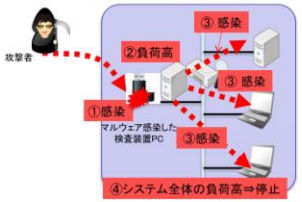
半導体分野のインシデント事例

●2011年に、日本の国内大手半導体メーカでUSBメモリを経由して、品質検査を行う検査装置へマルウェアが感染した。
●感染により、検査プロセス処理の負荷が異常に高まり、本来不良品として判定すべきものがそのまま検出されずに通ってしまう不具合が発生した。さらに感染元が分からず、感染が飛び火し、最終的には生産ラインが停止した。

半導体工場

出典：写真は参考情報（WEBRONZA）

マルウェア挙動解析



ウクライナの大規模停電

- 2015年12月23日にウクライナでサイバー攻撃による大規模停電（電力会社2-3社、影響人数 約22万人、停電時間3時間程度）が発生した。
- 当初はBlackEnergy3と呼ばれるマルウェアにより、監視制御システムのサーバのハードディスクが破壊されたことにより停電が発生したと報道されていたが、ハードディスクの破壊が停電に直結することは考えにくい。
- その後、リモート制御により（30カ所、110万ボルト級変電所7か所、35万ボルト級変電所23か所）のブレーカー遮断がなされたことが判明した。（BlackEnergy3の関与は不明）
- ウクライナ政府は、ICS-CERTに調査を要請し、ICS-CERTは以下の調査結果を発表した。
  1. 約22万5千人の顧客に影響が及んだ。
  2. VPN接続を介して電力会社の監視制御システムへアクセスが行われていた。
  3. 一連の攻撃にBlackEnegryが初期のアクセス手段として用いられたかどうかは定かではない。


http://styknews.info/novyny/ns/2015/12/23/frankivsk-na-pivgodyny-zalyshyvsia-bez-svitla-foto

一般家庭に及ぶ攻撃

boingboing / ANDREA JAMES / 8:20 AM FRI DEC 2, 2016

DDoS attack on Finnish automated buildings disabled heating controls

When the heat goes out during Finnish winter, it's a matter of life and death, so when two automated buildings controlled by Valtia systems suffered DDoS attacks that shut off the heat, Finns were understandably alarmed about the new threat.
Via Metropolitan.fi

時期　2016年10月頃(詳細不明)

場所　フィンランド　ラッペーンランタ

事象　自動制御されている建物少なくとも二棟のヒーティングシステムが停止。

原因　遠隔監視・制御しているValtia社のDNSサーバーがDDOS攻撃をうけたため。

同時期の気温は氷点下のため、人的被害の出る可能性もあった。

http://boingboing.net/2016/12/02/ddos-attack-on-finnish-automat.html

ホテルでのサイバーインシデント

高級ホテルでランサムウェア被害、宿泊客を部屋から閉め出し

オーストリアの高級ホテルで電子キーシステムがランサムウェアに感染し、宿泊客が自分の部屋に入れなくなった。攻撃者は、ビットコインで1500ユーロの身代金を要求していた。

[岡本玲子、ITmedia]

109 | 166 | 166 | 9 | 25 | 14

"現代の魔法使い"落合陽一氏が語るビジネスのデジタル化
富士通の最新オールフラッシュアレイは速いだけではない！

オーストリアの高級ホテルで客室のカードキーを発行するシステムなどがランサムウェアに感染し、宿泊客が部屋から閉め出される事件が起きた。欧州の英語ニュースサイト「The Local Europe」が1月28日付で伝えた。


オーストリアの4つ星ホテル「Romantik Seehotel Jaegerwirt」（公式Webページより）

記事によると、オーストリアの4つ星ホテルRomantik Seehotel Jaegerwirtで電子キーシステムがランサムウェアに感染した。同ホテルがサイバー攻撃を受けたのは今回が3度目だったという。

客室の扉はカード式のキーを使って施錠と開錠を行う仕組みだったが、サイバー攻撃に遭ってこのカードキーのシステムがダウンしたため、宿泊客は自分の部屋に入れなくなった。新しいカードキーのプログラムもできなくなったという。

http://www.itmedia.co.jp/enterprise/articles/1701/31/news068.html

電力システムに対する攻撃

'Russia hacking code' found on Vermont utility computer

31 December 2016 | US & Canada

An electrical company in the US state of Vermont says it has found malware code allegedly used by Russian hackers on one of its company laptops.

The Burlington Electric Department **said it had taken "immediate action to isolate"** the computer, which was not connected to the electrical grid.

The government alerted them to the "Grizzly Steppe" code on Thursday.

時期　2016年12月
(米国大統領選挙 11月)

場所　米国　バーモント州
バーリントン・エレクトリック・デパートメント社
(電力会社)

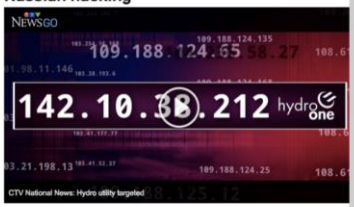
事象　社内ラップトップPCよりロシアのハッカーが使用しているとされるマルウェアを発見。電力網には接続されていなかった。発見後、直ちにネット環境から隔離。

GRIZZLY STEPPE
同時期に行われていたロシアのサイバー攻撃につけられた名称

出典：http://www.bbc.com/news/world-us-canada-38479179

電力システムに対する攻撃

Exclusive: IP address at Ontario power utility linked to alleged Russian hacking



CTVNews.ca Staff
Published Tuesday, January 3, 2017 6:28PM EST
Last Updated Wednesday, January 4, 2017 8:05AM EST

U.S. Homeland Security and the FBI have warned that Ontario's main electricity distributor may have been the target of malicious Russian cyber-activity.

時期　2016年12月
(米国大統領選挙 11月)

場所　カナダ　オンタリオ州
ハイドロ・ワン社
(送電・配電会社)

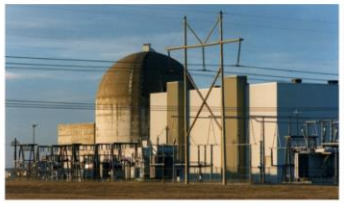
事象　ハイドロ・ワン社の使用しているIPアドレスの一つがロシアのサイバー攻撃に関連するものの一つだった。ここを基点に、電力網にサイバー攻撃を仕掛けることも可能であった。

出典：http://www.ctvnews.ca/canada/exclusive-ip-address-at-ontario-power-utility-linked-to-alleged-russian-hacking-1.3226290

電力システムに対する攻撃

Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say

By NICOLE PERLROTH JULY 6, 2017



The Wolf Creek Nuclear power plant in Kansas in 2000. The corporation that runs the plant was targeted by hackers. David Eulitt/Capital Journal, via Associated Press

Since May, hackers have been penetrating the computer networks of companies that operate nuclear power stations and other energy facilities, as well as manufacturing plants in the United States and other countries.

時期　2017年7月6日の記事

情報源
米国 国土安全保障省
F.B.I

内容
カンサス州の　Wolf Creek 原子力運営会社の情報システム系ネットワークがハッキングされた。
制御系システムに侵入された痕跡は無い。
将来の攻撃に向けた調査と推定。

出典：https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html

電力システムに対する攻撃


THE TIMES

Russia-backed hackers try to hijack Britain's power supply

Hackers backed by the Russian government have attacked energy networks running the national grid in parts of the UK, *The Times* has learnt.

時期
2017年7月15日の記事

発信者
Ireland's Electricity Supply Board (ESB)

内容
ロシアのGRUが関与するハッカー集団が、北アイルランドの送電システムに侵入。実害は無かったが、停電等の混乱を狙ったと考えられている。
従業員宛の標的型メールが確認されている。

電力システムに対する攻撃


Hacks 'probably compromised' UK industry

18 July 2017 · Technology

Some industrial software companies in the UK are "likely to have been compromised" by hackers, according to a document reportedly produced by British spy agency GCHQ.

A copy of the document from the National Cyber Security Centre (NCSC) - part of GCHQ - was obtained by technology website Motherboard.

A follow-up by the BBC indicated that the document was legitimate.

出典）http://www.bbc.com/news/technology-40642962
https://motherboard.vice.com/en_us/article/9kwpfa/gchq-says-hackers-have-likely-compromised-uk-energy-sector-targets

時期　2017年7月18日の記事

発信者
National Cyber Security Centre (NCSC)

内容
英国の複数の制御系システムを利用する企業が、国家レベルの組織が支援する敵対的ハッカー集団によって攻撃されている。

また、複数のエネルギー関連企業や製造業企業のIPアドレスが上記ハッカー集団に乗っ取られている。

この様な攻撃は英国に限られたものではなく、全世界的に行われている。

TV局に対する攻撃


How France's TV5 was almost destroyed by 'Russian hackers'

By Gordon Corera
Security correspondent, BBC News

10 October 2016 · Technology

TV5MONDE

TV5Monde's TV station, website and social media accounts were all hit in April 2015

A powerful cyber-attack came close to destroying a French TV network, its director-general has told the BBC.

http://www.bbc.com/news/technology-37590375

時期　2015年4月8日

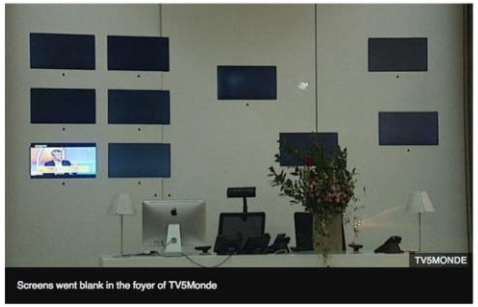
場所　フランス　TV5MONDE
(テレビ会社)

事象　午後8時に放送している12チャンネル全てが停止。翌朝5時に1チャンネル復旧。翌朝には完全復旧。

同時に同社のフェイスブック等もハッキングされる。

TV局に対する攻撃

"We were a couple of hours from having the whole station gone for good."



Screens went blank in the foyer of TV5Monde

http://www.bbc.com/news/technology-37590375

TV局に対する攻撃

How France's TV5 was almost destroyed by 'Russian hackers'

By Gordon Corera
Security correspondent, BBC News

10 October 2016 | Technology

A powerful cyber-attack came close to destroying a French TV network, its director-general has told the BBC.

当初、ISのサイバー攻撃と考えられたが、後にロシアのハッカーによるものと判明。
(2015年1月　シャルリー・エブド襲撃事件)

この攻撃は、非常に洗練されたもので、最初のネットワークへの侵入は2015年1月23日。

7つの方法を使って侵入したことが判明しており、そのうちの一つはTV5のスタジオから遠隔操作を行うオランダにあるお天気カメラと判明。

広がるサイバー攻撃ビジネス

プロによる安価なDDOSサービス

料金	
1～4時間	:1時間2ドル
5～24時間	:1時間4ドル
24～72時間	:1時間5ドル
1か月	:1000ドル

最大級のWebサイト・フォーラム・ゲームサービスを攻撃できます。
代金をいただく前にテストをいたします。
ただし、サービスの性質上返金はいたしません

https://2ogmrlfzdthnwkez.onion.to/

- サイバー攻撃下請けやサイバー攻撃ツールレンタル業者までいる闇市場
- 需要者は、サイバー軍やその下請け企業、犯罪集団やサイバーマフィア、テロ集団など

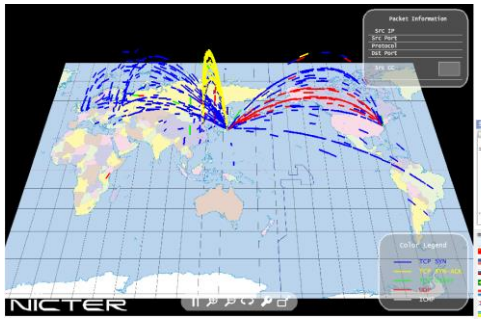
http://www.mcafee.com/de/resources/white-papers/wp-cybercrime-exposed.pdf/

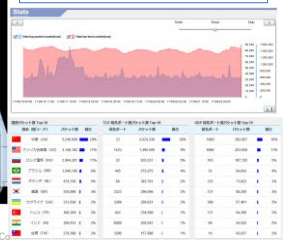
制御システムを標的にしたサイバー攻撃事例

- 攻撃手法も高度技術を使用しており、組織的サイバー攻撃兵器としても開発し、取引されている。
- 対策を考えるには、攻撃対象、攻撃武器、侵入経路、攻撃内容、被害状況などの具体的情報が必要となる。

	2008	2010	2014	2014	2015	2016.8～
発生場所	トルコ	イラン	ドイツ	韓国	ウクライナ	イラン
攻撃対象	石油パイプライン	核燃料施設	製鉄所	原子力発電所	電力変電所	製油所 天然ガス基地など
攻撃武器	不明	Stuxnet	トロイの木馬	外部操作を可能にしたマルウェア	スピアフィッシングメールで感染	不明 サイバー攻撃ではないかと疑われている
侵入経路	監視カメラの通信ソフト	USBメモリ	電子メールの添付ファイル	インターネットからの侵入	インターネットからの侵入	不明
攻撃内容	パイプ管圧への過剰な負荷	遠心分離機への過剰な負荷	溶鉱炉の異常停止	マルウェアを使った遠隔操作	UPSを攻撃	不明
被害状況	パイプライン爆発	遠心分離機を破壊	生産設備の損傷	実被害なし	広いエリアで6時間停電	石油貯蔵タンク爆発 火災（10月）

日本を攻撃するサイバー攻撃





http://www.nicter.jp/#
出展元：NICTER 観測レポート

日本を攻撃したサイバー攻撃件数
- 2011年　約45.4億件
- 2012年　約77.8億件
- 2013年　約128.8億件
- 2014年　約 256億6千万件
- 2015年　約 545億1千万件
- 2016年　約1281億件

日本を攻撃するサイバー攻撃

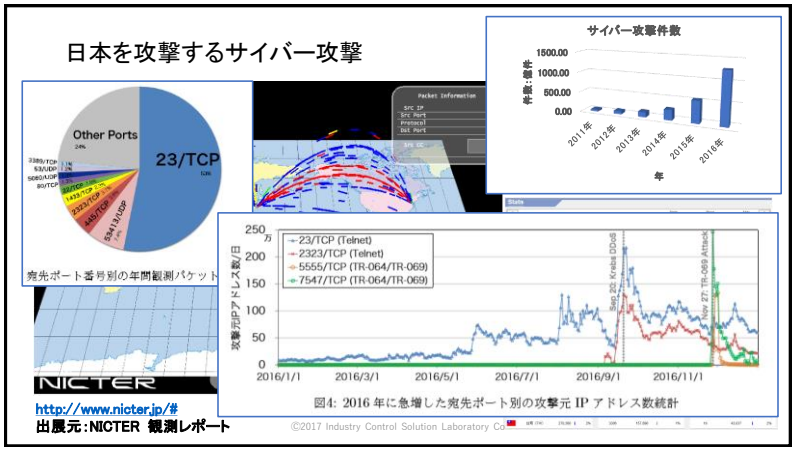


図4: 2016 年に急増した宛先ポート別の攻撃元 IP アドレス数統計

http://www.nicter.jp/#
出展元：NICTER 観測レポート

日本を攻撃するサイバー攻撃

表2: 各ピーク時の攻撃元国分布

9/20 (23/TCP or 2323/TCP)			11/27 (7547/TCP or 5555/TCP)		
国	#IPs	割合	国	#IPs	割合
ブラジル	456,778	約 21%	ブラジル	1,206,589	約 49%
ベトナム	283,997	約 13%	イラン	334,510	約 14%
インド	225,457	約 10%	イギリス	272,590	約 11%
中国	190,843	約 9%	トルコ	187,296	約 8%
ロシア	129,979	約 6%	チリ	84,755	約 3%
インドネシア	98,752	約 4%	イタリア	83,816	約 3%
コロンビア	82,806	約 4%	アイルランド	53,869	約 2%
メキシコ	49,605	約 2%	タイ	40,418	約 2%
トルコ	44,161	約 2%	アルゼンチン	34,861	約 1%
アルゼンチン	43,779	約 2%	インド	32,123	約 1%
その他	593,654	約 27%	その他	138,675	約 6%

図4: 2016 年に急増した宛先ポート別の攻撃元 IP アドレス数統計

http://www.nicter.jp/#
出展元：NICTER 観測レポート

©2017 Industry Control Solution Laboratory Co.

サイバーセキュリティ対策の重要性

国内で起きている事故

自動車工場	•現場サポート業者が持ち込んだPCから工場内ネットワークにマルウェア侵入。PC50台に感染 •10日間操業停止⇒1200台出荷できず：年間売り上げから30億円以上が無くなる
半導体製造工場	•現場装置のアップデート作業で持ち込んだデバイスから工場内ネットワークにマルウェア侵入 •1か月間操業停止⇒年間売り上げから340億円が無くなる。
石油精製工場	•MESのネットワークにマルウェアが侵入 •2週間操業停止⇒2週間分の出荷減
工作機械が並ぶ精密機械製造工場	•マルウェアが工場内ネットワークに侵入 •セキュア改善するまでは、年に数回数週間ずつ操業停止
ゴミ焼却場	•従業員が持ち込んだ携帯電話の充電中にインターネットと接続。マルウェアが侵入 •6日間操業停止
高速道路管制システム	•インターネットにつながるPCからマルウェアが侵入し、USBメモリ経由で管制システムに感染 •設備総入れ替え

サイバーインシデントが発生する都度に出てくる損失

何が問題か

- 年間計画している売り上げが減る。
  - 操業停止している期間の売り上げが無くなる。
- 復旧作業の為にコスト増
  - 緊急対応コスト
    - マルウェア判定：専門家に依頼
    - 洗浄作業：
    - 回復作業：ベンダを呼びだして作業依頼
  - セキュア改善対策コスト
    - インシデント検知システム
    - セグメント設計改造
    - ゾーン設計改造
    - インシデント対応トレーニング

いずれにしろ、やることになる投資

マルウェア（Malware）

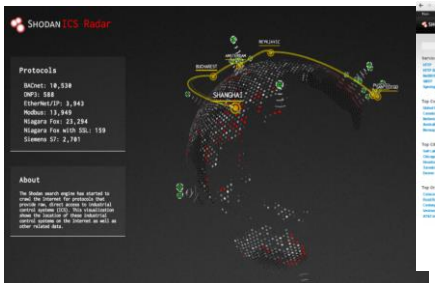
マルウェア：悪意をもって作られたソフトウェア

マルウェア（Malware）

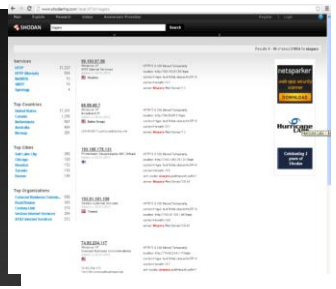
- 意図としない動きをするソフト
  - ウイルス
    - Worm
  - スクリプトウイルス
    - PLC Blaster Worm
    - Black Energy
  - ワーム
- 開発や設計時の裏口機能を悪用する
  - バックドア
- キー入力のロガー機能をIDやパスワード情報搾取に利用される
  - キーロガー
- ダウンロードを利用してマルウェアを送り込み、それをServer化させる
  - トロイの木馬
  - バックドア型、パスワード窃盗型、クリッカー型、ダウンローダー型、ドロッパー型、プロキシ型
- WordやExcelのマクロファイルとして挿入され、意図としない動きをする
  - マクロウイルス
- ブートセクタを書き換える。再起動すると意図としないところへ飛んで行って戻らない
  - ブートセクタウイルス
    - Shamoon
  - ミスリーディングアプリケーション
    - Stuxnet
- C&C Server Connect
  - インターネットにつながる装置を検索してC&C Serverにアップ
  - SHODAN Censys
- クライムウェア
  - 犯罪行為を目的に作られたソフト
- スケアウェア
  - ユーザーを脅してお金を奪う目的のソフト
  - Ransomware
- スパイウェア
  - ユーザーの情報を自動的に指定されたところへ送る
  - Havex（Dragonfly）
- 悪質なアドウェア
  - 無料ソフトに情報収集目的の機能を入れたもの
- ユーザーが意図としない操作や動きをさせるソフト

悪用されるSHODAN

- インターネットにつながる制御装置や機械を検索して、市場や通信仕様条件別に分類し、サイバー攻撃に必要な情報を提供していることになる。

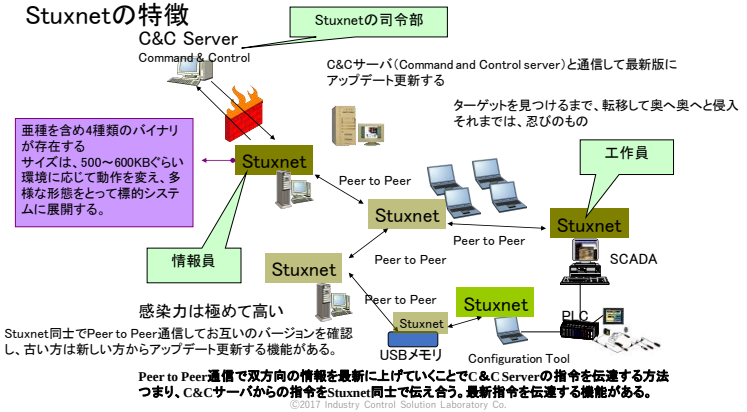


出典元　https://ics-radar.shodan.io/

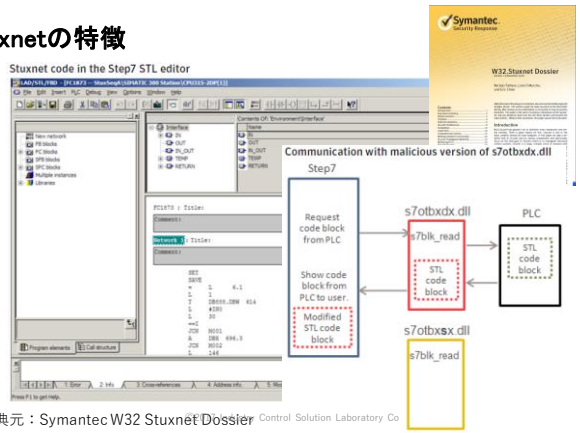


出典元　www.shodanhq.com

Stuxnetの特徴



Stuxnetの特徴



出典元：Symantec W32 Stuxnet Dossier

Black Energy

- 2015年12月23日ウクライナの電力が6時間程度停電
- スピアフィッシングメールによるインターネットからの侵入でUPSを攻撃

Black Energyについて

- 初期のBlack Energy
  - DDOS攻撃の単純なものであった。
- Black Enery2
  - 2010年インストーラーが組み込まれた。
  - 2011年UAC（User Account Control：ユーザーアクセス制御）をバイパスするインストーラーが追加
    新しいバージョンのWindowsでも旧来のアプリケーションが使えるようにMicrosoftが提供しているフレームワークを用いて、Black Energy 2が昇格したコード実行権限を獲得することが可能になった。
  - 2013年　64ビットドライバーをサポート
- Black Energy3
  - 2014年先行バージョンよりも高度な機能が組み込まれており、より巧妙化

Black Energy3の分析

Black Energy3のプラグイン＊

- **fs.dll－ファイルシステム操作**
- **si.dll－システム情報取得 "BlackEnergy Lite"**
- **jn.dll－寄生する感染機能付マルウェア**
- **ki.dll－キーロガー**
- **ps.dll－パスワード盗聴**
- **ss.dll－スクリーンショット**
- **ve.dll－ネットワーク検出、リモート実行**
- **tv.dll－チームビューワー（遠隔操作ツール）**
- **rd.dll－シンプルな偽物の "リモートデスクトップ"**
- **up.dll－マルウェアのアップデート**
- **do.dll－Windoweアカウントの一覧表示**
- **be.dll－システムハードウェア、BIOS、Windowe情報の照会**
- **dstr.dll－システムの破壊**
- **scan.dll－ネットワークスキャン**

- この新しいバージョンには、ドライバが組み込まれておらず、ビルド番号のフォーマットはタイムスタンプがあり、高度な保護の仕組みを数多く備えています。
- これらの内部保護機能には、仮想環境、アンチデバッグ機能、コード全体の継続的なチェックに対する防衛策を備えており、他のセキュリティ機能や対策を検出した場合にはプログラムを消去します。

特徴

- 侵入技術が高度
- 送られた環境でマルウェアが生成・成長する
- 感染が速い
- 攻撃手法が高度

WanaCry／Goldeneye／Petya／Bad Rabbit＋Ransomware

- WanaCryは、2017年4月25日にトレンドマイクロが発見。Windowsの脆弱性をついたRansomwareによる攻撃で、150ヵ国で25万台以上の被害が出た。日本でも6000件以上の被害が出たと報告がある。
- 多くの医療施設が機能停止。重要インフラ／製造業の企業でも被害を受ける。

出典元：ICS-CERT

Goldeneye

脆弱性があるWindowsのSMB：Windows Server Message Blockを攻撃するエクスプロイトEternalBlueを利用した攻撃。
既にMS17-010のパッチが出ているが、このパッチ処理をしていないWindowsが狙われている。

リモートシステムを利用した攻撃

- サイバーセキュリティコンサルが分らないようにコンサルサポートシステムを利用して、企業機密を搾取したり、マルウェアを送り込む。
  - ロシアのハッカー集団が米国国防省をサポートしているカスペルスキー社のサイバーセキュリティサポートシステムを利用して軍事機密情報を盗もうとした。
  - 日本のサイバーセキュリティコンサルSky社のコンサルサポートシステムSKYSEAの脆弱性を利用して企業機密情報を盗まれる。
- 医療機関や工場の設備をリモートサポートしているシステムを利用して、リモートサポート顧客の設備にマルウェアを感染させる。
  - WannaCryの被害
    - 病院の電源設備断、手術ができない、透析装置が動かない、集中治療室の機能停止、患者情報喪失
    - 自動車製造ライン停止
    - 交通管制システム情報Serverダウン
    - 工場の製造生産情報・品質情報・設備情報喪失など

SKY SEAの脆弱性：CVE-2016-7836

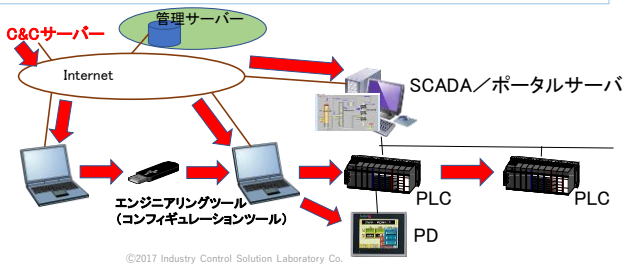
- IT資産管理サービスを提供しているSKY SEAに、脆弱性があることが2016年12月21日に報告アップされ、それ以降3回の脆弱性報告さなされた。

出典元：CVEサイト

PLC Blaster Worm

攻撃方法

- インターネット上のC&Cサーバーから侵入する。
- コンフィギュレーションツールやポータルサーバー製品経由でコントローラに侵入する。
- コントローラのレジスタをアクセスしたり、プロファイルを書き換えたり差し替えたりする。



PLC Blaster Worm：コントローラに仕込まれるマルウェア

- PLCのコンフィギュレーションツールやPLCにつながるポータルツールからWormをPLCに送り込み、PLCからPLCに感染させることもできる。PLCをネット上のC&Cサーバーの支配下におくこともできる。

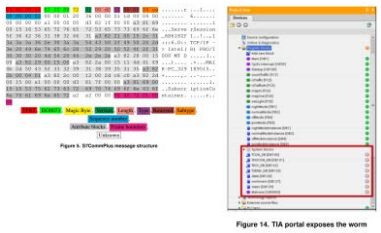


Figure 14. TIA portal exposes the worm

資料は、Asia Black Hat 2016の発表PDFより引用

対策は、IEC62443-4-1の更新版でも検討課題。

Vendor	Product	Ethernet	Transfer TCP/UDP	TCP/IP Functions
Siemens	S7-300	Ja	Ja	Ja
Siemens	S7-400	Ja	Ja	Ja
Siemens	S7-1200	Ja	Ja	Ja
Siemens	S7-1500	Ja	Ja	Ja
Mitsubishi Electric	MELSEC iQ-R	Ja	Ja	Ja
Mitsubishi Electric	MELSEC iQ-F	Ja	Ja	Ja
Mitsubishi Electric	MELSEC-Q	Ja	Ja	Ja
Mitsubishi Electric	MELSEC-L	Ja	Ja	Ja
Mitsubishi Electric	MELSEC-F	Ja	Ja	Nein
Mitsubishi Electric	MELSEC-QS/WS	Ja	Ja	Nein
Schneider Electric	Modicon Easy M	Nein	Nein	Nein
Schneider Electric	Modicon M	Ja	Ja	Nein
Schneider Electric	Modicon LM	Ja	Ja	Nein
Schneider Electric	Modicon Premium	Ja	Ja	Nein
Schneider Electric	Modicon Quantum	Ja	Ja	Nein
Schneider Electric	Preventa XPS Quantum	Ja	Ja	Nein
Rockwell Automation	ControlLogix	Ja	Ja	Ja
Rockwell Automation	CompactLogix	Ja	Ja	Ja
Rockwell Automation	MicroLogix	Ja	Ja	Ja
Rockwell Automation	SmartGuard 600	Ja	Ja	Nein
Rockwell Automation	SLC 500	Ja	Ja	Ja
Rockwell Automation	PLC-5	Ja	Ja	Ja
Rockwell Automation	GuardPLC	Ja	Ja	Nein
Rockwell Automation	Micro800	Ja	Ja	Nein

制御システムの攻撃方法

- **定常時／非定常時の操作ミス（誤判断・誤操作）を誘発する**
  - **制御ネットワークを使えなくする**
    - **ネットワークのServerかPCからDOS攻撃を加えて通信エラーを起こす**
  - **現場で発生していないアラームを発報させる**
    - **DCSやSCADAの監視制御のアラームデータに新しい警報を追加**
    - **過去起きたアラームを再度表示**
  - **現場で発生しているアラームを監視画面に表示させない**
    - **アラームデータが上がってきてもデータベースに書き込まない**
    - **アラームデータを消去**
- **直接攻撃**
  - **SCADAの制御動作をスローダウンもしくは機能停止させる**
    - **SCADA ServerにWormを送り込みフル稼働させる：Worm**
    - **使用しているファイルを暗号化する：Ransomware**
    - **制御データがSCADAに上がってこなくする：通信ドライバを消去、データベースを消去**
  - **制御コントローラを機能停止する**
    - **コントローラの正常レジスタをOFFにする：PLC Blaster Worm**
    - **コントローラの停止レジスタをONにする：PLC Blaster Worm**
  - **実際にメカニックストレスを与える**
    - **制御コントローラにストレスデマンドを送り込む：Stuxnet**

要因

- 冗長化システムは、ハードウェア故障対策しか考慮されていない。（サイバー攻撃についての冗長化になっていない。）
- コンフィギュレーションツールのセキュリティチェックをしていない
- インシデント検知機能が無い
- インシデント対応トレーニングをしていない
- 回復作業のトレーニングが実施されていない（すべてベンダ任せ）
- 脆弱性情報が管理されていない
- パッチバージョン管理をしていない

安全のFTA（Fault Tree Analysis）に制御システムセキュリティ・リスクを加える