2023 CYBER THREATS FOR THE INDUSTRIAL SECTOR

Part 2

ROOT LEVEL RESOURCES

KEY TECHNIQUES OF THE MITRE ATTACK ®

TACTIC	MITRE ID	TECHNIQUE
INITIAL ACCESS	T1190	Exploit Public-Facing Application
	T1566.001	Phishing: Spearphishing Attachment
	T1566.002	Phishing: Spearphishing Link
	T1566	Phishing
	T1078.002	Valid Accounts: Domain Accounts
EXECUTION	T1203	Exploitation for Execution
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1106	Native API
	T1204	User Execution
	T1559	Inter-Process Communication
PERSISTENCE	T1547	Boot or Logon Autostart Execution
	T1574	Hijack Execution Flow
	T1547.002	Hijack Execution Flow: DLL Side-Loading
	T1078.002	Valid Accounts: Domain Accounts
	T1078.003	Valid Accounts: Local Accounts
PRIVILEGE ESCALATION	T1547	Boot or Logon Autostart Execution
	T1574	Hijack Execution Flow
	T1055	Process Injection
	T1548	Abuse Elevation Control Mechanism
	T1547.002	Hijack Execution Flow: DLL Side-Loading
DEFENSE EVASION	T1027	Obfuscated Files or Information
	T1140	Deobfuscate/Decode Files or Information
	T1574	Hijack Execution Flow
	T1562	Impair Defenses
	T1036	Masquerading
CREDENTIAL ACCESS	T1552.001	Unsecured Credentials: Credentials In Files
	T1555.003	Credentials from Password Stores: Credentials from Web Browsers
	T1056	Input Capture
	T1003.001	OS Credential Dumping: LSASS Memory
	T1003.003	OS Credential Dumping: NTDS
DISCOVERY	T1082	System Information Discovery
	T1057	Process Discovery
	T1087	Account Discovery
	T1135	Network Share Discovery
	T1069	Permission Groups Discovery
LATERAL MOVEMENT	T1210	Exploitation of Remote Services
	T1570	Lateral Tool Transfer
	T1550.002	Use Alternate Authentication Material: Pass the Hash
	T1021.001	Remote Services: Remote Desktop Protocol
COLLECTION	T1560.001	Archive Collected Data -> Archive via Utility
	T1005	Data from Local System
	T1560	Archive Collected Data
	T1119	Automated Collection
	T1602	Data from Configuration Repository
COMMAND AND CONTROL	T1105	Ingress Tool Transfer
	T1071.001	Application Layer Protocol: Web Protocols
	T1102	Web Service
	T1071	Application Layer Protocol
	T1573.002	Encrypted Channel: Asymmetric Cryptography
EXFILTRATION	T1041	Exfiltration Over C2 Channel
	T1020	Automated Exfiltration
	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage
	T1537	Transfer Data to Cloud Account
	T1485	Data Destruction
	T1489	Service Stop

Intelligence services attacking the industrial sector

ROOT LEVEL RESOURCES

Traditional hackers, as well as competing companies and countries engaged in corporate espionage, are more and more often targeting manufacturers. The motives for such attacks range from financial gain and revenge to competitive intelligence for strategic breakthroughs.

Existing manufacturing systems were developed when cybersecurity had not been seen as an urgent problem, so the main focus of manufacturing technology was on productivity and production security (not in an informational context). This has led to large security gaps. The growing complexity of such systems drove the development of complex and large network-wide, highly specialized infrastructures. In most cases, these systems are not operated and managed by IT specialists, but by manufacturing experts.

Such trends, combined with the integration of IT and operations, have generated an enormous area for attack, which is very difficult to manage and defend.

APT41

This elaborate malware campaign has gone undetected at least since 2019. It targeted tech and **manufacturing companies** in North America, Europe, and Asia. Over the years of scouting and identifying valuable data, this hacker group managed to steal hundreds of gigabytes of information.

They targeted intellectual property developed by the victims, including confidential documents, diagrams, formulas, drawings, and confidential data related to manufacturing.

They also collected information that could be used for future cyberattacks, such as information about the target company's business units, network architecture, user accounts and credentials, employees' emails, and customer data.

Specialists are highly confident in attributing the attack and Operation **CuckooBees** to the **APT41** group.

The original entry point into the organization occurred because of multiple vulnerabilities in the enterprise resource planning (ERP) organizational platform.

Attackers used a new custom rootkit – **WINNKIT**. Its goal is to act as a kernel-mode agent, interacting with the user-mode agent and intercepting TCP/IP requests, addressing directly to the network card.

Dark Halo

In spring 2022, a file was uploaded to VirusTotal from Sri Lanka disguised as Roshan_CV.iso and containing a malicious payload associated with the new **Brute Ratel C4 (BRc4)** tool (compilation date May 17, 2022). We should note that not a single antivirus tool has qualified this file as malicious.

Specialists managed to disclose some of the BRc4 infrastructure and samples. Moreover, experts found that at least 3 organizations in North and South America had been affected by the tool. Including a **major textile manufacturer in Mexico**.

The sample was downloaded following the same pattern used by the **DarkHalo** group to spread Cobalt Strike to victims' machines in recent attacks. The attack execution chain can be represented as a scheme:

Roshan_CV.ISO → *Roshan-Bandar_CV_Dialog. LNK* → *cmd.exe* → *OneDriveUpdater.exe* → *version.dll* → *OneDrive.Update*

The final code loaded into memory is the Brute Ratel C4 tool.

Lazarus

North Korean group **Lazarus** used payloads in KMSAuto and the trojanized KeePass for their complex attacks.

In the spring of 2022, there was an attack on an **industrial equipment supplier in the Philippines** involving a similar trojanized KeePass malware.[1].

The purpose of this software is to load the encrypted Mimikatz from the file system, which required three parameters:

- The location of the encrypted Mimikatz in the file system
- The key to decrypt it
- The doubly base64-encoded argument for Mimikatz, which could look like *privilege:: debug,lsadump::dcsync/ domain:<DOMAIN>/all /csv.*

Specialists categorize these files as a set of Lazarus-specific tools.

In the fall of 2022, experts discovered that Lazarus had installed one of its payloads in *C:\ProgramData\KMSAutoS\KMSAuto.bin* and disguised it as a well-known Windows activation tool.

The useful payload is the VMProtect executable, not KMSAuto.

The Philippine vendor we mentioned regarding the trojanized KeePass app also fell victim to this payload. The hackers exploited a crack that was already present on the victim's system in the same folder that is usually prescribed to be excluded from anti-virus checks. So, for security, piracy is not only a risk of getting malicious software, but also evading detection.

APT40

The Chinese pro-government hackers **APT40** are not slowing down and continue to attack various organizations in Australia. The conflation of targets related to Australian government affairs as well as offshore energy production in the South China Sea occurred in the latest campaign. The victims were the **world's heavy industry manufacturers** who maintain a fleet of wind turbines in the South China Sea.

Manufacturers received phishing emails with URLs that redirected them to a malicious website posing as an Australian news agency. In turn, the website's landing page delivered the malicious JavaScript ScanBox[2] code to its targets.

In isolated cases, ScanBox was delivered from websites that were subjected to strategic web compromise (SWC) attacks, when malicious JavaScript code was injected into legitimate sites. This is how an attacker controls a malicious site and delivers malicious code to users.

Aggah

In the summer of 2022, the **Aggah** group sent phishing emails to industrial organizations in Taiwan and South Korea.

One of the mailings was on behalf of a food delivery company, FoodHub. The email contained information about the order and an attachment Purchase order 4500061977,pdf.ppam. The recipient was the Taiwanese company Fon-Star International Technology Inc.

Другими жертвами подобных писем стали:

- **CSE group** Taiwanese manufactory
- **FomoTech** Taiwanese engineering company
- **Hyundai Electric** Korean energy company

The sent attachment contained an obfuscated macro that MSHTA uses to execute a Jscript posted on a compromised legitimate Indian hotel website.

WordPress hosted most of the legitimate compromised sites used to host the malicious payload. Jscript checks for debugging tools, and then refers to another compromised site of an Afghan food delivery company.

First, hackers download and execute a PowerShell script, which is used to check the status of anti-virus tools (checking for Windows Defender, ESET, or their lack.) Based on the results, different loaders will be used to inject Warzone into a legitimate process.

Tropic Trooper

The group uses xPack to attack financial institutions and **manufacturing companies**.

This backdoor allows hackers to remotely run WMI commands and mount shared resources via SMB to send them data from C&C servers. Attackers also used malicious software to browse the web pages as a proxy server to disguise their IP address.

One of the attacks carried out by the group left in the compromised network of a Taiwanese manufacturing organization **for 175 days**.

The original infection vector is currently unclear. Experts suggest that the hackers used a web application or service, as in one of the attacks the MSSQL service was used to execute system commands.

Exforel

China's **Daxin** has remained undetected for **more than 10 years**. Security experts discovered the tool's deployment in government organizations, as well as organizations operating in the telecommunications, transportation, and **manufacturing sectors**.

Daxin comes in a rare malware format - the Windows kernel driver. It implements advanced communication features that provide a high degree of stealth and allow you to communicate with infected computers in highly secure networks **where a direct connection to the Internet is not available**.

Daxin can also broadcast its messages over the network of infected computers in the attacked organization. Attackers can choose any path through infected computers and send a command offering to make the requested connection.

Malicious software avoids running its own network services. Instead, it abuses legitimate services running on infected computers.

ROOT LEVEL RESOURCES

FORECASTS

The number of encryption attacks will increase

- Computers of engineers and software developers will be used more and more often as an entry point for attacks since they provide access to computer-aided process control systems and feature elevated privileges.
- Exploitation of old vulnerabilities, including those related to routers, will remain the main vector of attack, since not all companies are proactive in installing security patches.
- Supply chain and trusted relationship attacks, where hackers gain access to production facilities by compromising software or telecommunications providers, are expected to increase.

1 KeePass — a free and open-source password manager that helps users manage their passwords securely.

2 ScanBox Primer: ScanBox – a JavaScript-based web exploration and exploitation platform that allows attackers to profile victims and deliver malicious software to selected targets.

3 Warzone RAT – An informative C++ stealer that supports privilege escalation, keylogging, Remote Shell, file download and execution, file handling, persistence, credential theft.