Trustwave SpiderLabs

Manufacturing Sector **Deep Dive**

Methods of Targeting and Breaching

Contents

Overview

The manufacturing industry is integral to building economies and bolstering innovation. This industry, which is one of the most profitable industries globally, is seeing massive growth because of the Fourth Industrial Revolution, which prioritizes digitization to bolster productivity, improve data and analytics, and support agility and sustainability. However, when organizations integrate advanced technologies into their operations, they face exposing their systems and machines to a slew of cybersecurity threats and risks.

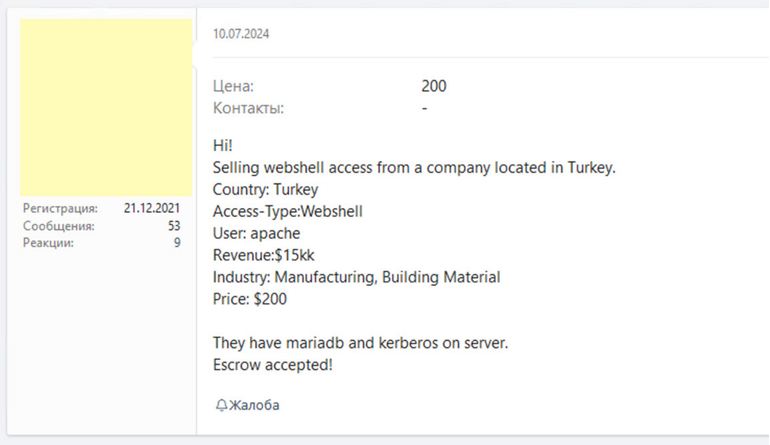
In this report, the Trustwave SpiderLabs team tackles the different ways in which the manufacturing industry is targeted and breached by threat actors. This report looks at the most recent cyberattacks waged against Trustwave clients in the manufacturing industry, including web shells, vulnerability exploitation, and social engineering attacks, especially phishing.

This report is a supplemental report to the of the 2025 Trustwave Risk Radar Report: Manufacturing Sector, a broader and more comprehensive report that analyzes the manufacturing sector's major threats and trends.

Web Shells

Web shells are lightweight malicious scripts that attackers upload to compromised servers, providing a hidden doorway to the system. These tools are highly prevalent on Dark Web marketplaces, often marketed as a cost-effective and stealthy way to maintain unauthorized access to corporate networks. Web shells are particularly dangerous for manufacturing companies, as they enable attackers to infiltrate production environments, gather sensitive information, and establish a persistent presence for extended operations.

Once installed, a web shell allows attackers to execute arbitrary commands, upload and download files, escalate privileges, and even move laterally within a company's infrastructure to reach more sensitive systems.



[redacted]

Регистрация:	21.12.2021
Сообщения:	53
Реакции:	9

10.07.2024

Цена:	200
Контакты:	-

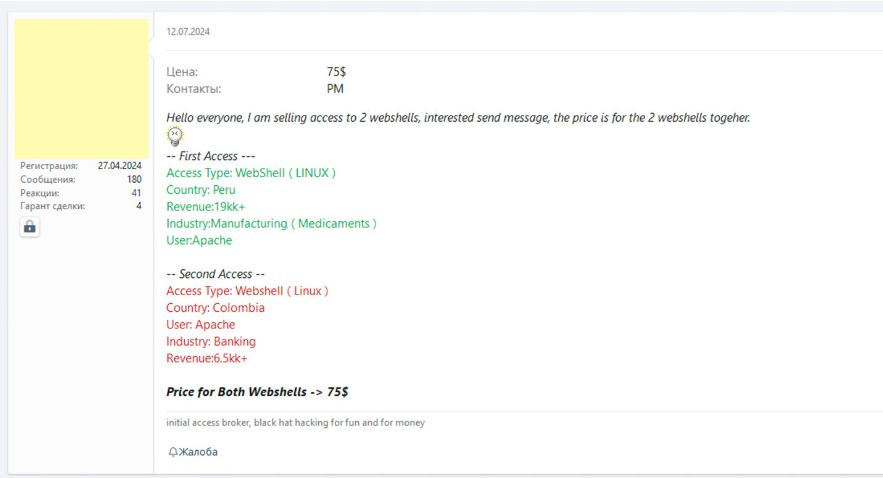
Hi!
Selling webshell access from a company located in Turkey.
Country: Turkey
Access-Type:Webshell
User: apache
Revenue:$15kk
Industry: Manufacturing, Building Material
Price: $200

They have mariadb and kerberos on server.
Escrow accepted!

Жалоба

Figure 1. A threat actor offers web shell access to a Turkish manufacturing company

For attackers, web shells offer several advantages. They are relatively simple to deploy, especially in environments where vulnerabilities in web applications or outdated software exist. Web shells are also discreet, as they often mimic legitimate traffic, making them difficult to detect without robust monitoring tools. Additionally, web shells serve as an entry point for further exploits, such as deploying ransomware, stealing intellectual property, or disabling critical machinery. These capabilities make web shells an invaluable asset for attackers targeting manufacturing companies.



[redacted]

Регистрация: 27.04.2024
Сообщения: 180
Реакции: 41
Гарант сделки: 4

12.07.2024

Цена: 75$
Контакты: PM

Hello everyone, I am selling access to 2 webshells, interested send message, the price is for the 2 webshells togeher.

-- First Access ---
Access Type: WebShell (LINUX)
Country: Peru
Revenue:19kk+
Industry:Manufacturing (Medicaments)
User:Apache

-- Second Access --
Access Type: Webshell (Linux)
Country: Colombia
User: Apache
Industry: Banking
Revenue:6.5kk+

Price for Both Webshells -> 75$

initial access broker, black hat hacking for fun and for money

Figure 2. A Dark Web advertisement claims to sell access to two web shells for affordable price.

Web shell prices on the Dark Web vary based on the target's value, the level of access provided, and the method used to compromise a server. Access to servers belonging to high-value manufacturing companies, especially those tied to operational technology (OT) systems, commands a premium, while less critical targets are cheaper.

Advanced web shells with features such as privilege escalation or lateral movement capabilities are more expensive than basic ones. The exploitation method also plays a role — web shells installed using zero-day vulnerabilities are pricier than those relying on widely known flaws. Market dynamics, such as supply and demand, and the geographic or industrial significance of the target further influence pricing.

However, web shells are not without limitations. Their functionality is often restricted to the compromised server, and additional effort may be required to pivot to other parts of the network. Modern security measures, such as web application firewalls and advanced intrusion detection systems, can identify and neutralize web shell activity. Despite these defenses, the rise of automated attack tools and vulnerabilities in legacy systems ensure that web shells remain a popular option among cybercriminals.

Vulnerability Exploitation

All vulnerability data included in this report was collected via Shodan.

Manufacturing organizations had 4,370 unique vulnerabilities (out of a total of 24,920) publicly exposed on the Internet. 3,843 of these vulnerabilities are critical vulnerabilities, and 3,532 were listed in the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerability (KEV) list, as seen in Table 1.

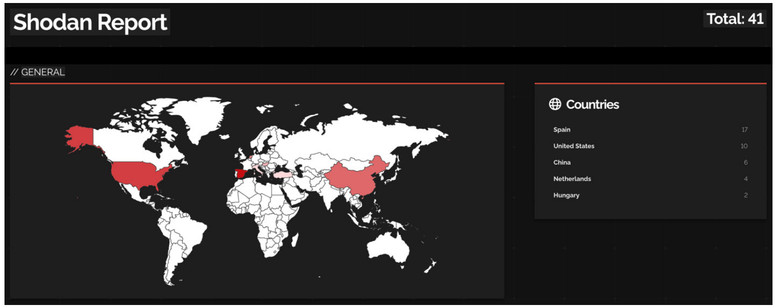
CVE ID	Description	Count
CVE-2021-40438	A Server-Side Request Forgery (SSRF) vulnerability in Apache HTTP Server versions up to 2.4.48. Exploiting this flaw allows attackers to force the server to forward requests to arbitrary destinations, potentially accessing internal systems.	1,603
CVE-2023-44487	Known as the "HTTP/2 Rapid Reset" vulnerability, this flaw allows attackers to exploit the HTTP/2 protocol to cause denial-of-service (DoS) conditions by rapidly resetting streams, leading to server resource exhaustion. In October 2023, multiple organizations reported large-scale DDoS attacks leveraging this vulnerability, prompting widespread advisories and patches.	836
CVE-2019-0211	A privilege escalation vulnerability in Apache HTTP Server versions 2.4.17 to 2.4.38. A local user with the ability to run scripts could execute arbitrary code with the privileges of the Apache server process.	471
CVE-2024-4577	A critical remote code execution vulnerability affecting PHP versions 5.x and onwards on Windows servers configured in CGI mode. Improper input validation allows attackers to execute arbitrary code on the server.	381
CVE-2020-0796	Also known as "SMBGhost," this is a remote code execution vulnerability in Microsoft's Server Message Block 3.1.1 (SMBv3) protocol. An attacker could exploit this flaw to execute code on the target server or client.	60
CVE-2012-1823	A vulnerability in PHP-CGI-based setups that allows remote attackers to execute arbitrary code or cause a denial of service via query strings, leading to code injection.	57
CVE-2014-0160	Known as "Heartbleed," this is a severe vulnerability in OpenSSL versions 1.0.1 through 1.0.1f. It allows attackers to read sensitive memory contents, potentially exposing confidential data.	41
CVE-2019-11043	A remote code execution vulnerability in PHP-FPM when used with NGINX. Improper handling of certain FastCGI requests can lead to arbitrary code execution.	31
CVE-2015-1635	A remote code execution vulnerability in the HTTP.sys component of Microsoft Windows. An attacker could send a specially crafted HTTP request to execute arbitrary code on the target system.	22
CVE-2019-0708	Dubbed "BlueKeep," this is a remote code execution vulnerability in Microsoft's Remote Desktop Services. Unauthenticated attackers can connect via RDP and execute arbitrary code on the target system.	15

Table 1. Vulnerabilities with respect to the CISA known exploited vulnerabilities catalog

Publicly Accessible Industrial Control Systems (ICS)

Industrial Control Systems (ICSs) are essential in manufacturing, automating processes to enhance efficiency and productivity. They include systems such as supervisory control and data acquisition (SCADA), distributed control systems (DCSs), and programmable logic controllers (PLCs), which monitor and control industrial operations.

However, connecting ICS to networks exposes them to cybersecurity threats. Common issues include vulnerabilities in outdated software, unauthorized access due to weak authentication, and susceptibility to malware and ransomware attacks. A quick search showed 41 publicly exposed ICS systems.



Spain	17
United States	10
China	6
Netherlands	4
Hungary	2

Figure 3. Shodan search for publicly accessible ICS systems

Recent data indicates a significant rise in cyberattacks targeting ICS. In 2022, there was an 87% increase in ransomware attacks on industrial organizations, with a 35% rise in the number of ransomware groups targeting ICS and operational technology systems.

A notable incident is the discovery of new malware capable of terminating engineering processes in ICS environments. Identified in August 2024, this malware targets Siemens engineering workstations, posing significant risks to industrial operations.

To mitigate these risks, manufacturers should implement robust cybersecurity measures, including regular system updates, strong authentication protocols, and continuous monitoring, to safeguard ICS from potential attacks.

Credential Stealer Marketplaces

Credential stealer log marketplaces on the Dark Web are thriving hubs where cybercriminals trade stolen login details for various systems, including corporate email accounts, and operational technology systems. These credentials are often harvested using malware — credential stealers, designed to extract stored passwords from infected devices or through phishing campaigns targeting unsuspecting employees. Once stolen, credentials are listed on marketplaces where buyers can filter by company size, geographic location, or the type of access offered, making it easy to acquire specific entry points into manufacturing organizations.

For example, consider one of the most well-known American automobile brands globally, which has over 15,000 records referencing the ford.com domain in credential stealer logs available for sale for the last year.

Here is a sample of a credential stealer log, where pluses are signed data available in the log:

```
faust.idp.ford.com
Login: +
Password: +
Cookie: -

ford.onwingspan.com
Login: +
Password: +
Cookie: +

web.gsdb2.ford.com
Login: +
Password: +
Cookie: -
```

Credential stealer logs pose significant risks by providing login credentials, session cookies, and browser details that attackers can use to bypass security measures including multi-factor authentication (MFA). Cybercriminals exploit them for account takeovers, unauthorized transactions, and access to corporate systems, with high-value targets such as executives being particularly vulnerable. Additionally, these credentials are often resold on Dark Web marketplaces, increasing their potential for misuse.

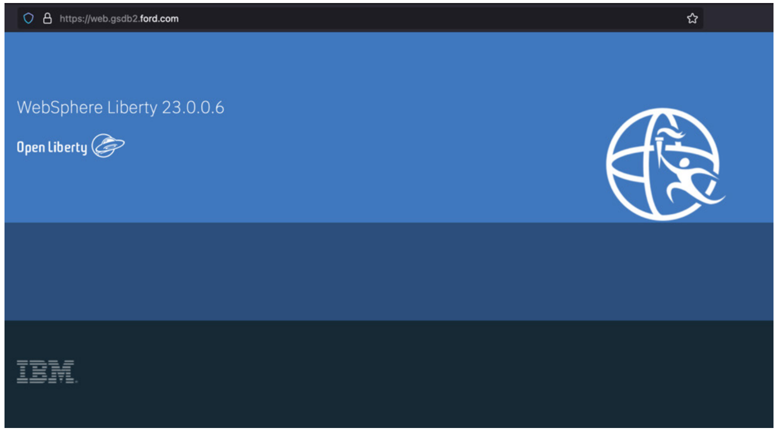
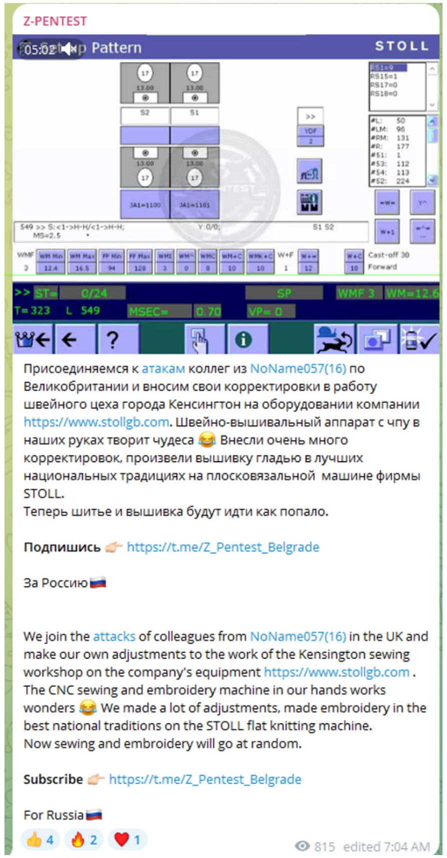


Figure 4. The landing page for the web[.]gsdb2[.]ford[.]com domain, mentioned in the credential stealer log

For the manufacturing industry, the data available on these marketplaces poses a significant threat. Credentials sold may include access to enterprise resource planning (ERP) systems, supply chain management software, or OT networks used to control production lines. Attackers can exploit these credentials to disrupt manufacturing operations, exfiltrate sensitive intellectual property, or deploy ransomware. In addition to production delays, stolen access can compromise sensitive designs, trade secrets, or contracts with suppliers and clients, leading to significant reputational and financial damage.



Присоединяемся к атакам коллег из NoName057(16) по Великобритании и вносим свои корректировки в работу швейного цеха города Кенсингтон на оборудовании компании https://www.stollgb.com. Швейно-вышивальный аппарат с чпу в наших руках творит чудеса 😂 Внесли очень много корректировок, произвели вышивку гладью в лучших национальных традициях на плосковязальной машине фирмы STOLL.
Теперь шитье и вышивка будут идти как попало.

Подпишись 👉🏻 https://t.me/Z_Pentest_Belgrade

За Россию🇷🇺

We join the attacks of colleagues from NoName057(16) in the UK and make our own adjustments to the work of the Kensington sewing workshop on the company's equipment https://www.stollgb.com .
The CNC sewing and embroidery machine in our hands works wonders 😂 We made a lot of adjustments, made embroidery in the best national traditions on the STOLL flat knitting machine.
Now sewing and embroidery will go at random.

Subscribe 👉🏻 https://t.me/Z_Pentest_Belgrade

For Russia🇷🇺

👍 4 🔥 2 ❤️ 1 815 edited 7:04 AM

Figure 5. Pro-Russian hacking group claims interrupting a sewing manufacturer’s machines

The consequences of such breaches are far-reaching. If a manufacturing company becomes a victim of credential theft, attackers can sabotage production processes, infiltrate supply chain networks, or even manipulate OT systems, potentially causing physical damage to machinery or creating safety hazards. Moreover, compromised credentials may provide a foothold for attackers to move laterally within the network, targeting critical data or deploying destructive malware.

To mitigate these risks, manufacturing companies must prioritize robust password hygiene, implement MFA, and regularly monitor for compromised credentials on the Dark Web. Employee training to recognize phishing attempts, combined with advanced endpoint detection systems, can also reduce the likelihood of credential theft. By taking proactive measures, manufacturers can minimize their exposure to the threats posed by credential stealer marketplaces and protect their critical operations.

Noteworthy Phishing Campaigns

Phishing Attacks via Email

File-Sharing Phishing Attack

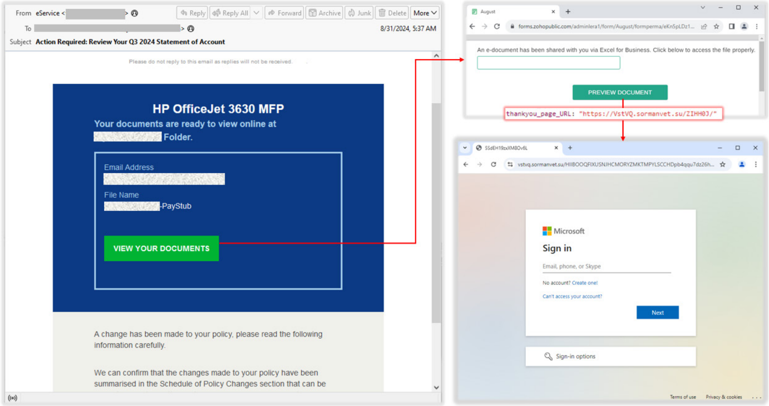
This phishing campaign exploits the trust associated with file-sharing services. Attackers mimic email alerts of internal systems or applications including printer services and commonly used external platforms such as WeTransfer.

The following phishing samples were received by our manufacturing sector clients and detected by our email security product MailMarshal.

Fake Printer Notification Email:

The document supposedly being shared is a pay stub, a document issued by the employer on each pay day. Clicking the "VIEW YOUR DOCUMENTS" will launch a page from Zoho Forms, an online forms platform.

With Zoho Forms, the user can be forwarded to a "Thank You" page once the form is submitted. This Zoho feature has been repurposed in this campaign by having content that redirects to a Microsoft phishing page associated with the Tycoon Phishing-as-a-Service (PaaS) platform.



From eService <[redacted]>
To [redacted]>
8/31/2024, 5:37 AM
Subject Action Required: Review Your Q3 2024 Statement of Account

Please do not reply to this email as replies will not be received.

HP OfficeJet 3630 MFP
Your documents are ready to view online at [redacted] Folder.

Email Address
[redacted]
File Name
[redacted]-PayStub

A change has been made to your policy, please read the following information carefully.

We can confirm that the changes made to your policy have been summarised in the Schedule of Policy Changes section that can be

forms.zohopublic.com/adminlera1/form/August/formperma/eKn5pLDz1...

An e-document has been shared with you via Excel for Business. Click below to access the file properly.

```
thankyou_page_URL: "https://VstVQ.sormanvet.su/ZIHH0J/"
```

vstvq.sormanvet.su/HIIBOOQFIXUSNJHCMORYZMKTMPYLSCCHDpb4qqu7dz26h...

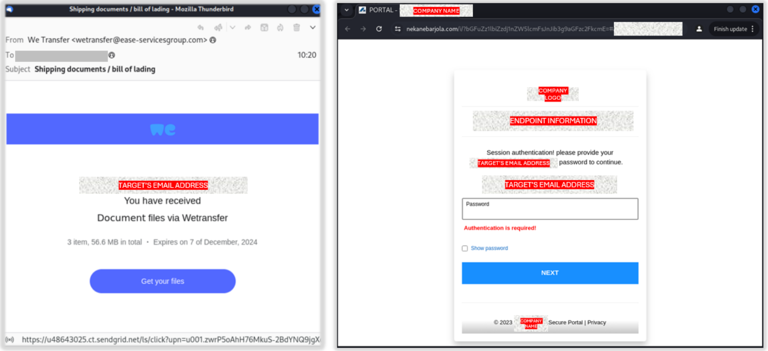
Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?

Figure 6. A sample of a fake printer notification email that leads to a phishing page

Fake Bill of Landing (BOL) Email:

Manufacturers frequently use a BOL document, which is a legal document issued by a carrier, that serves as both a contract and a receipt for transferring goods to a receiver. In this phishing sample, the phishers impersonate WeTransfer and notify users of a supposed shared BOL document.

Clicking the link leads users to a phishing website that is designed to appear as an internal secure portal to obtain a user's account password. To further enhance the deception, the phishing site dynamically displays the logo of the recipient company and additional endpoint information including OS, browser, time stamp, and location.



Shipping documents / bill of lading - Mozilla Thunderbird

From We Transfer <wetransfer@ease-servicesgroup.com>

To [redacted] 10:20

Subject **Shipping documents / bill of lading**

TARGET'S EMAIL ADDRESS

You have received

Document files via Wetransfer

3 item, 56.6 MB in total · Expires on 7 of December, 2024

https://u48643025.ct.sendgrid.net/ls/click?upn=u001.zwrP5oAhH76MkuS-2BdYNQ9jgX

PORTAL - COMPANY NAME

nekanebarjola.com/i/?bGFuZz1lbiZzdj1nZW5lcmFsJnJib3g9aGFzc2FkcmE=# [redacted]

COMPANY LOGO

ENDPOINT INFORMATION

Session authentication! please provide your TARGET'S EMAIL ADDRESS password to continue.

TARGET'S EMAIL ADDRESS

Password

Authentication is required!

□ Show password

© 2023 COMPANY NAME Secure Portal | Privacy

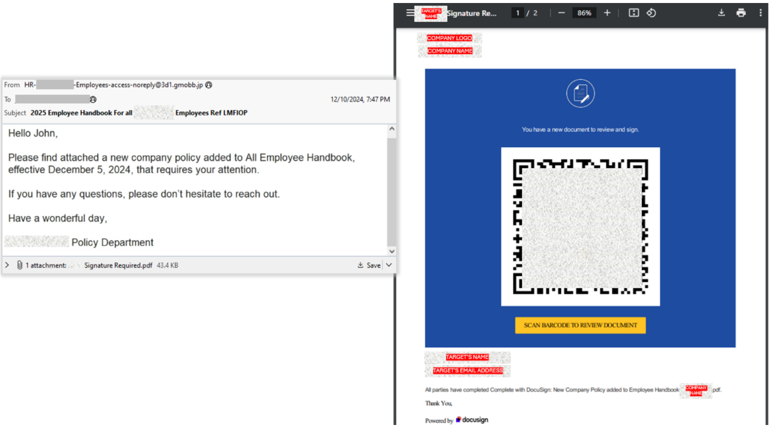
Figure 7. A sample of a fake BOL document that leads to a phishing site that dynamically shows a user's logo and endpoint information

HR-Themed Phishing Attack

We have observed an increase in phishing emails imitating HR communications, particularly toward the end of 2024.

The PDF attachment is disguised as a revised employee handbook for the upcoming year. To make the attachment appear realistic, the contents of the PDF file are aligned to the theme of the email. The PDF is cloaked as a document from the e-signature platform DocuSign and employee data such as username, company name, and company logo are incorporated in the PDF file.

The PDF attachment contains a QR code leading to a phishing page utilizing the Mamba phishing kit, another PaaS capable of adversary-in-the-middle (AiTM) attacks.



From HR-[redacted]-Employees-access-noreply@3d1.gmobb.jp

To [redacted] 12/10/2024, 7:47 PM

Subject **2025 Employee Handbook For all [redacted] Employees Ref LMFIOP**

Hello John,

Please find attached a new company policy added to All Employee Handbook, effective December 5, 2024, that requires your attention.

If you have any questions, please don't hesitate to reach out.

Have a wonderful day,

[redacted] Policy Department

1 attachment: [redacted] Signature Required.pdf 43.4 KB

TARGET'S NAME Signature Re... 1 / 2 86%

COMPANY LOGO

COMPANY NAME

You have a new document to review and sign.

TARGET'S NAME

TARGET'S EMAIL ADDRESS

All parties have completed Complete with DocuSign: New Company Policy added to Employee Handbook COMPANY NAME .pdf.

Thank You,

Powered by docusign

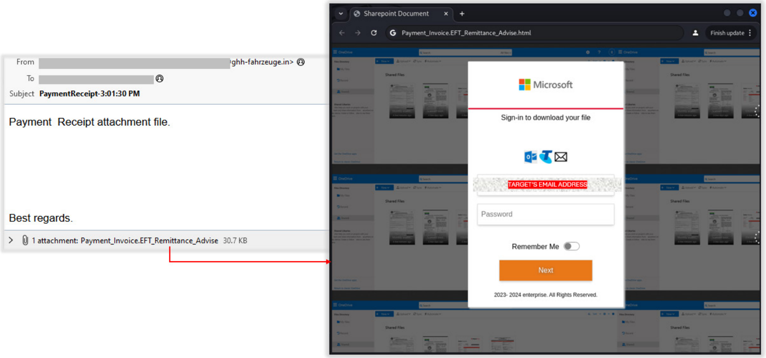
Figure 8. A fake employee handbook cloaked as a DocuSign PDF contains a malicious QR code that leads to a phishing page

Payment Confirmation Phishing Attacks

Payment and invoice lures are among the most common themes observed in phishing campaigns that target the manufacturing sector. One kind of attack that employs this lure is payment confirmation fraud, where cybercriminals send fake payment receipts or invoices for goods and services that the recipient did not purchase.

Payment Receipt Phishing Attack:

This phishing email sample claims to be from **GHH Fahrzeuge GmbH**, another manufacturing company in the machinery field. This simple email contains an HTML attachment masked as a payment receipt. Opening the attachment yields to a standalone credential phishing page designed to look like a Microsoft login page.



From [redacted]ghh-fahrzeuge.in>

To [redacted]

Subject **PaymentReceipt-3:01:30 PM**

Payment Receipt attachment file.

Best regards.

1 attachment: Payment_Invoice.EFT_Remittance_Advise 30.7 KB

Sign-in to download your file

TARGET'S EMAIL ADDRESS

Password

Remember Me

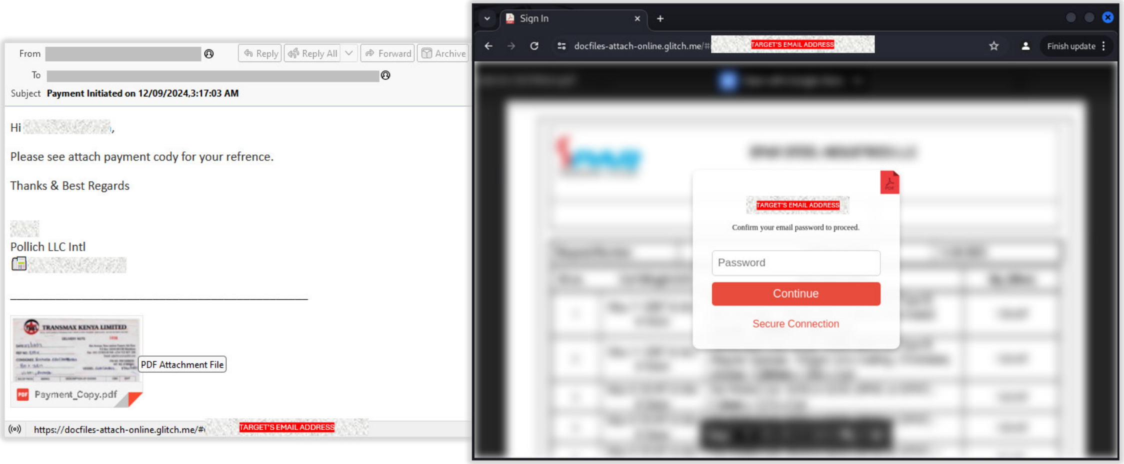
2023- 2024 enterprise. All Rights Reserved.

Figure 9. A fake payment receipt with a malicious HTML attachment that leads to a phishing page

Image-Based Phishing Attack:

This phishing sample involves multiple manufacturing companies. The email was sent from a compromised email address belonging to a manufacturing company. The attacker then opted to impersonate a different manufacturing company named Pollich LLC Intl. The message was sent to one of our manufacturing sector customers.

The threat actors embedded an image of a receipt and anchored the phishing link to it. Clicking the fake receipt will direct the user to a phishing page hosted on Glitch, a web hosting platform with free plan offerings.



From [redacted]

To [redacted]

Subject **Payment Initiated on 12/09/2024,3:17:03 AM**

Hi [redacted],

Please see attach payment cody for your refrence.

Thanks & Best Regards

[redacted]
Pollich LLC Intl
[redacted]

https://docfiles-attach-online.glitch.me/# TARGET'S EMAIL ADDRESS

docfiles-attach-online.glitch.me/# TARGET'S EMAIL ADDRESS

TARGET'S EMAIL ADDRESS

Confirm your email password to proceed.

Password

Figure 10. A phishing link anchored to a fake payment receipt image attachment that leads to a Glitch-hosted phishing page

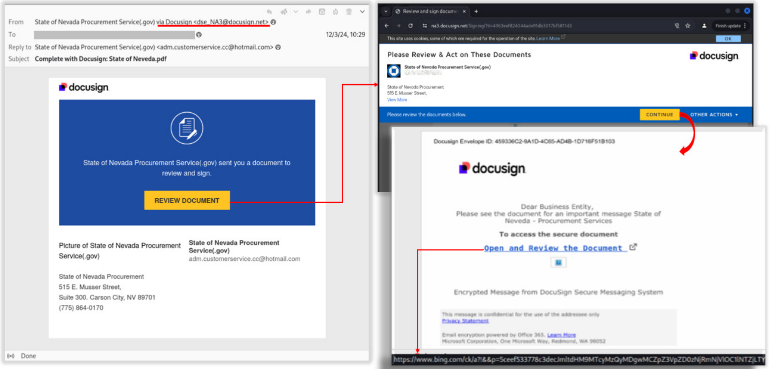
Phishing Attacks Abusing Legitimate E-Signature Platforms

Fake Government Procurement Document Sent Via DocuSign

We have observed multiple phishing campaigns using DocuSign to send phishing messages. Clicking the link will direct users to a legitimate DocuSign envelope that contains a phishing link.

In the email sample below, the threat actor posed as “State of Nevada Procurement Services” and used the DocuSign platform to trick victims into thinking that the malicious document was a legitimate government procurement document.

The link used Bing as a redirector and redirected users to a fake login page associated with the Tycoon 2FA PaaS.



From State of Nevada Procurement Service(.gov) via Docusign <dse_NA3@docusign.net>
To [redacted] 12/3/24, 10:29
Reply to State of Nevada Procurement Service(.gov) <adm.customerservice.cc@hotmail.com>
Subject **Complete with Docusign: State of Neveda.pdf**

docusign

State of Nevada Procurement Service(.gov) sent you a document to review and sign.

REVIEW DOCUMENT

Picture of State of Nevada Procurement Service(.gov)

State of Nevada Procurement Service(.gov)
adm.customerservice.cc@hotmail.com

State of Nevada Procurement
515 E. Musser Street,
Suite 300. Carson City, NV 89701
(775) 864-0170

Done

Review and sign docume
na3.docusign.net/Signing/?ti=4963eef824044ade91db3017bf581143
This site uses cookies, some of which are required for the operation of the site. Learn More OK

Please Review & Act on These Documents docusign

State of Nevada Procurement Service(.gov)
[redacted]

State of Nevada Procurement
515 E. Musser Street,
View More

Please review the documents below. CONTINUE OTHER ACTIONS ▾

Docusign Envelope ID: 459336C2-9A1D-4C65-AD4B-1D716F51B103

docusign

Dear Business Entity,
Please see the document for an important message State of Neveda - Procurement Services

To access the secure document

Open and Review the Document

Encrypted Message from DocuSign Secure Messaging System

This message is confidential for the use of the addressee only
Privacy Statement

Email encryption powered by Office 365. Learn More
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

https://www.bing.com/ck/a?!&&p=5ceef533778c3decJmltdHM9MTcyMzQyMDgwMCZpZ3VpZD0zNjRmNjVlOC1lNTZjLTY

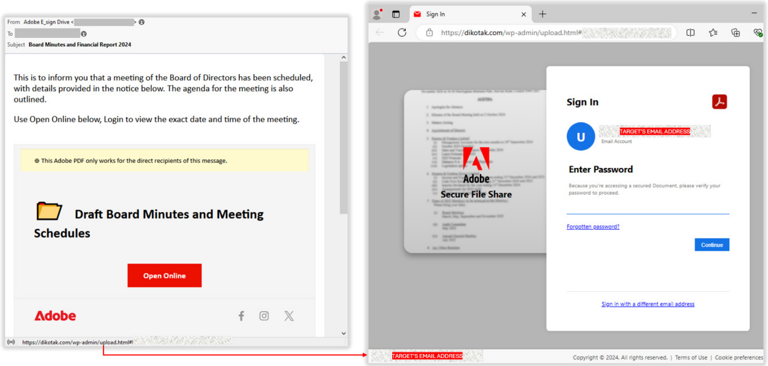
Figure 11. Threat actors abused the DocuSign platform to distribute a fake government procurement document that leads to a fake login page

Trustwave SpiderLabs has previously observed this tactic with the Rockstar 2FA.

E-Signature Platform Lure: Adobe Acrobat Sign

The phishing email below was designed to mimic an email notification from Adobe Acrobat Sign, an e-signature platform by Adobe. The sender claims to share board meeting minutes and schedules from the said platform. A closer look at the URL reveals /wp-admin/, an indicator that the page is likely hosted on a compromised WordPress site. This is a common tactic used in phishing attacks to host malicious content.

Clicking the link directs users to a credential harvesting page crafted to resemble the e-signature platform.



From Adobe E_sign Drive <[redacted]>
To [redacted]
Subject **Board Minutes and Financial Report 2024**

This is to inform you that a meeting of the Board of Directors has been scheduled, with details provided in the notice below. The agenda for the meeting is also outlined.

Use Open Online below, Login to view the exact date and time of the meeting.

⊕ This Adobe PDF only works for the direct recipients of this message.

Draft Board Minutes and Meeting Schedules

Open Online

Adobe

https://dikotak.com/wp-admin/upload.html#[redacted]

Sign In
https://dikotak.com/wp-admin/upload.html#[redacted]

Adobe
Secure File Share

Sign In

U [redacted] TARGET'S EMAIL ADDRESS
Email Account

Enter Password

Because you're accessing a secured Document, please verify your password to proceed.

Forgotten password?

Continue

Sign in with a different email address

[redacted] TARGET'S EMAIL ADDRESS

Copyright © 2024. All rights reserved. | Terms of Use | Cookie preferences

Figure 12. Fake Adobe Acrobat Sign email notification that leads to a phishing page hosted on a compromised WordPress site

Security Recommendations for Manufacturing Companies

- **Enhance Cybersecurity Posture:** Implement robust measures such as zero-trust architectures, MFA, and end-to-end encryption to minimize vulnerabilities.
- **Segment Networks:** Separate operational technology (OT) systems from IT networks to limit the spread of ransomware within an organization.
- **Conduct Regular Security Audits:** Identify and address vulnerabilities through frequent penetration testing and vulnerability assessments.
- **Invest in Employee Training:** Educate employees about phishing, social engineering, and other entry points commonly exploited by attackers.
- **Develop Incident Response Plans:** Create and test response protocols to ensure rapid recovery in case of an attack, minimizing downtime.
- **Collaborate and Share Intelligence:** Partner with industry peers, government agencies, and cybersecurity firms to share threat intelligence and best practices.
- **Adopt Supply Chain Risk Management:** Work closely with suppliers and partners to ensure they follow strong cybersecurity practices, reducing risks of third-party compromise.

By taking these steps, manufacturing companies can better safeguard their operations, protect intellectual property, and maintain resilience against evolving threats and risks.

For all of Trustwave SpiderLabs' research on the Manufacturing sector, please see the full series here.

Trustwave
SpiderLabs