

Table of contents

Overview

● Description	4
● Confidence	4
● Content	5

Entities

● Indicator	6
● Intrusion-Set	8
● Malware	9
● Attack-Pattern	10
● Country	14
● Region	15
● Sector	16

Observables

● IPv4-Addr	17
● Domain-Name	18

External References

● External References	19
-----------------------	----

Overview

Description

Proofpoint identified a financially motivated cybercriminal group known as TA547 targeting German organizations with emails delivering the Rhadamanthys information stealer malware. This was the first observation of TA547 using Rhadamanthys. The attack chain involved emails impersonating a German retail company containing LNK files that executed a PowerShell script to load and run the malware. The PowerShell script contained characteristics suggesting it may have been generated using a large language model tool. While the origin of malicious code does not impact detection, this provides insight into threat actors leveraging AI-generated content.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name

indscpm.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'indscpm.xyz']

Name

94.131.104.223

Description

```
**ISP:** STARK INDUSTRIES SOLUTIONS LTD **OS:** - ----- Services:
**22:** ~~~ SSH-2.0-OpenSSH_8.0 Key type: ssh-rsa Key:
AAAAB3NzaC1yc2EAAAADAQABAAQGCsWHAMkyI1pfFhIBigAGZdlXuNC5R2FAGE30TakKsod+3l
vMdIXe/lVoPsvNdc5eKKn1D+oJYRBInvBJ50iawzzNjkperxhjbby8CgMdkdt2uPdAKM9Z644pKZ
UPZVgeykVGeNVlJto7CiQGZvkdvZ91y/+8pXcGwVKO+j6+meRK//8llThWtIFwsud8Da+5V80/wv
OpNn2Qn6InvlTUZOsyqR4iFeSTyzCW65KrRvlzcl2wN/dTjnLgUAWSuDf6UCnB8yTSSrRsAp/isz
6hGVAXQMz9wwLdQgaDrQ8OJPxiNdrYTYvgSVVprf9NtzUH1Xhzl++e0z6/am/2cS45rQX03gA5E
UwzowKXkLjWzs3bgjNNVopggFXA/dqx6eUJOgdTbogNNvD86RfrxVyDVXdGuOPwWrlXpJSc6KtWI
T9yBFD6mt47HUdY8jF+PP0AF9rUD92QXqC59qu5HL/qAD/AjBt6y40378rNhRMLZ7Cha05eY8pn
diwUH2nIF6U= Fingerprint: 85:17:81:b0:c6:83:6c:7b:a1:15:44:92:65:d9:af:c8 Kex Algorithms:
curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384
```

```
ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha256
diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-
exchange-sha1 diffie-hellman-group14-sha1 kex-strict-s-v00@openssh.com Server Host
Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519
Encryption Algorithms: aes256-gcm@openssh.com chacha20-poly1305@openssh.com
aes256-ctr aes256-cbc aes128-gcm@openssh.com aes128-ctr aes128-cbc MAC Algorithms:
hmac-sha2-256-etm@openssh.com hmac-sha1-etm@openssh.com umac-128-
etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha2-256 hmac-sha1
umac-128@openssh.com hmac-sha2-512 Compression Algorithms: none zlib@openssh.com
```
----- **443:**` HTTP/1.1 200 OK Content-Type: text/html Server: Nginx Date:
Sun, 31 Mar 2024 14:51:34 GMT Content-Length: 614 `` HEARTBLEED: 2024/03/31 14:51:48
94.131.104.223:443 - SAFE ----- **10443:**` `` HEARTBLEED: 2024/04/08 14:02:04
94.131.104.223:10443 - SAFE -----
```

**Pattern Type**

stix

**Pattern**

[ipv4-addr:value = '94.131.104.223']

# Intrusion-Set

**Name**

TA547



# Malware

## Name

Rhadamanthys

# Attack-Pattern

## Name

T1059

## ID

T1059

## Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](<https://attack.mitre.org/techniques/T1059/004>) while Windows installations include the [Windows Command Shell](<https://attack.mitre.org/techniques/T1059/003>) and [PowerShell](<https://attack.mitre.org/techniques/T1059/001>). There are also cross-platform interpreters such as [Python](<https://attack.mitre.org/techniques/T1059/006>), as well as those commonly associated with client applications such as [JavaScript](<https://attack.mitre.org/techniques/T1059/007>) and [Visual Basic](<https://attack.mitre.org/techniques/T1059/005>). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](<https://attack.mitre.org/tactics/TA0001>) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](<https://attack.mitre.org/techniques/T1021>) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

**Name**

T1027

**ID**

T1027

**Description**

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](<https://attack.mitre.org/techniques/T1140>) for [User Execution](<https://attack.mitre.org/techniques/T1204>). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](<https://attack.mitre.org/techniques/T1027/010>) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](<https://attack.mitre.org/techniques/T1059>). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

**Name**

T1566

**ID**

T1566

**Description**

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

**Name**

T1204

**ID**

T1204

**Description**

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/

techniques/T1566). While [User Execution](<https://attack.mitre.org/techniques/T1204>) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](<https://attack.mitre.org/techniques/T1534>). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](<https://attack.mitre.org/techniques/T1219>), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](<https://attack.mitre.org/techniques/T1204>). For example, tech support scams can be facilitated through [Phishing](<https://attack.mitre.org/techniques/T1566>), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](<https://attack.mitre.org/techniques/T1219>). (Citation: Telephone Attack Delivery)

# Country

**Name**

Germany

# Region

**Name**

Western Europe

**Name**

Europe

# Sector

**Name**

Retail

**Description**

Distribution and sale of goods directly to the consumer.

**Name**

Manufacturing

**Description**

Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.



# IPv4-Addr

## Value

94.131.104.223

# Domain-Name

## Value

indscpm.xyz

# External References

- 
- <https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta547-targets-german-organizations-rhadamanthys-stealer>
- 
- <https://otx.alienvault.com/pulse/6616ff9eb99a8329eb508fd3>