Jan 22 2024

NETMANAGEIT

Intelligence Report

Russian threat group COLDRIVER expands its targeting of Western officials to include the use of malware

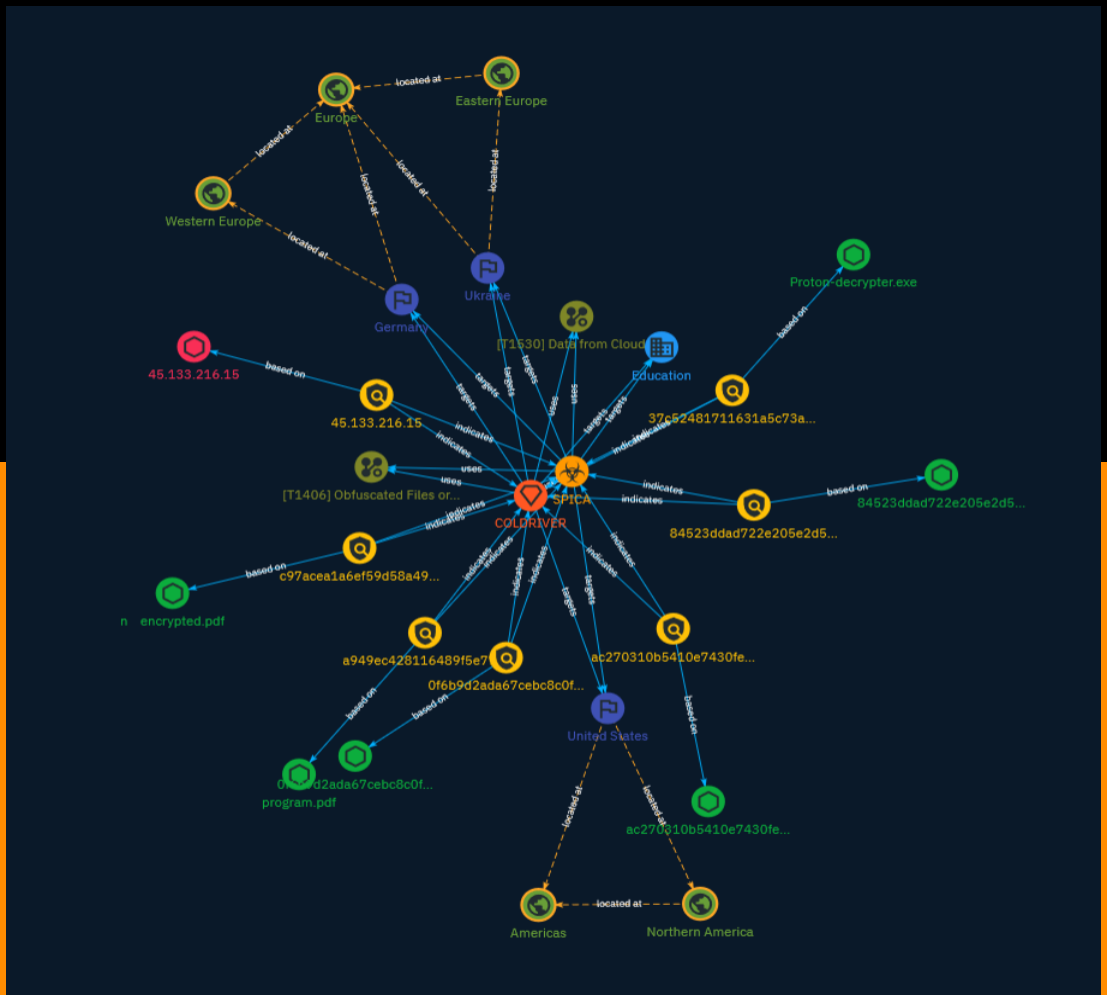

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Attack-Pattern 6
- Sector 8
- Indicator 9
- Intrusion-Set 13
- Region 14
- Country 15
- Malware 16

Observables

- StixFile 17
- IPv4-Addr 18

External References

- External References 19

Overview

Description

COLDRIVER's targeting of high profile individuals in NGOs, former intelligence and military officials and NATO governments is moving beyond credential phishing activities.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name

Data from Cloud Storage

ID

T1530

Description

Adversaries may access data from cloud storage. Many IaaS providers offer solutions for online data object storage such as Amazon S3, Azure Storage, and Google Cloud Storage. Similarly, SaaS enterprise platforms such as Office 365 and Google Workspace provide cloud-based document storage to users through services such as OneDrive and Google Drive, while SaaS application providers such as Slack, Confluence, Salesforce, and Dropbox may provide cloud storage solutions as a peripheral or primary use case of their platform. In some cases, as with IaaS-based cloud storage, there exists no overarching application (such as SQL or Elasticsearch) with which to interact with the stored objects: instead, data from these solutions is retrieved directly though the [Cloud API](https://attack.mitre.org/techniques/T1059/009). In SaaS applications, adversaries may be able to collect this data directly from APIs or backend cloud storage objects, rather than through their front-end application or interface (i.e., [Data from Information Repositories](https://attack.mitre.org/techniques/T1213)). Adversaries may collect sensitive data from these cloud storage solutions. Providers typically offer security guides to help end users configure systems, though misconfigurations are a common problem.(Citation: Amazon S3 Security, 2019) (Citation: Microsoft Azure Storage Security, 2019)(Citation: Google Cloud Storage Best Practices, 2019) There have been numerous incidents where cloud storage has been improperly secured, typically by unintentionally allowing public access to unauthenticated users, overly-broad access by all users, or even access for any anonymous person outside the control of the Identity Access Management system without even needing basic user permissions. This open access may expose various types of sensitive data, such as credit

cards, personally identifiable information, or medical records.(Citation: Trend Micro S3 Exposed PII, 2017)(Citation: Wired Magecart S3 Buckets, 2019)(Citation: HIPAA Journal S3 Breach, 2017)(Citation: Rclone-mega-extortion_05_2021) Adversaries may also obtain then abuse leaked credentials from source repositories, logs, or other means as a way to gain access to cloud storage objects.

Name

Obfuscated Files or Information

ID

T1406

Description

Adversaries may attempt to make a payload or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the device 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. Portions of files can also be encoded to hide the plaintext strings that would otherwise help defenders with discovery. Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled.(Citation: Microsoft MalLockerB)

Sector

Name
Education
Description
Public or private entities operating to facilitate learning and acquiring knowledge and skills, composed of infrastructures and services to host teachers, students, and administrative services related to this activity. This does not include research activities.

Indicator

Name
c97acea1a6ef59d58a498f1e1f0e0648d6979c4325de3ee726038df1fc2e831d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'c97acea1a6ef59d58a498f1e1f0e0648d6979c4325de3ee726038df1fc2e831d']
Name
a949ec428116489f5e77cefc67fea475017e0f50d2289e17c3eb053072adcf24
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a949ec428116489f5e77cefc67fea475017e0f50d2289e17c3eb053072adcf24']
Name

37c52481711631a5c73a6341bd8bea302ad57f02199db7624b580058547fb5a9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '37c52481711631a5c73a6341bd8bea302ad57f02199db7624b580058547fb5a9']

Name

0f6b9d2ada67cebc8c0f03786c442c61c05cef5b92641ec4c1bdd8f5baeb2ee1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0f6b9d2ada67cebc8c0f03786c442c61c05cef5b92641ec4c1bdd8f5baeb2ee1']

Name

45.133.216.15

Description

ISP: STARK INDUSTRIES SOLUTIONS LTD **OS:** None ---------- Hostnames: - vm1959787.stark-industries.solutions ---------- Domains: - stark-industries.solutions ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFMEHNxKimQjS2ECYuLxdAQT ii6j9iUrK4tB3J63yIQTvHf0iDB02iOmgs48D8y+4zcXOt5uI1TVHRu5glByLEE= Fingerprint: 36:e8:4b:22:9a:4d:e8:47:2a:58:de:7f:01:0e:c6:52 Kex Algorithms: curve25519-sha256 curve25519-

sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ```

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.133.216.15']

Name

84523ddad722e205e2d52eedfb682026928b63f919a7bf1ce6f1ad4180d0f507

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '84523ddad722e205e2d52eedfb682026928b63f919a7bf1ce6f1ad4180d0f507']

Name

ac270310b5410e7430fe7e36a079525cd8724b002b38e13a6ee6e09b326f4847

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = 'ac270310b5410e7430fe7e36a079525cd8724b002b38e13a6ee6e09b326f4847']

Intrusion-Set

Name
COLDRIVER

Region

Name
Europe
Name
Northern America
Name
Eastern Europe
Name
Western Europe
Name
Americas

Country

Name
Germany
Name
United States
Name
Ukraine

Malware

Name
SPICA

StixFile

Value
84523ddad722e205e2d52eedfb682026928b63f919a7bf1ce6f1ad4180d0f507
ac270310b5410e7430fe7e36a079525cd8724b002b38e13a6ee6e09b326f4847
c97acea1a6ef59d58a498f1e1f0e0648d6979c4325de3ee726038df1fc2e831d
37c52481711631a5c73a6341bd8bea302ad57f02199db7624b580058547fb5a9
a949ec428116489f5e77cefc67fea475017e0f50d2289e17c3eb053072adcf24
0f6b9d2ada67cebc8c0f03786c442c61c05cef5b92641ec4c1bdd8f5baeb2ee1

IPv4-Addr

Value
45.133.216.15

External References

- https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/
- https://otx.alienvault.com/pulse/65a975c11b1689cdd7554994