Jun 11 2023

NETMANAGEIT

Intelligence Report

APT-C-36 (Blind Eagle) Group Deploys LimeRAT Components Against Colombia

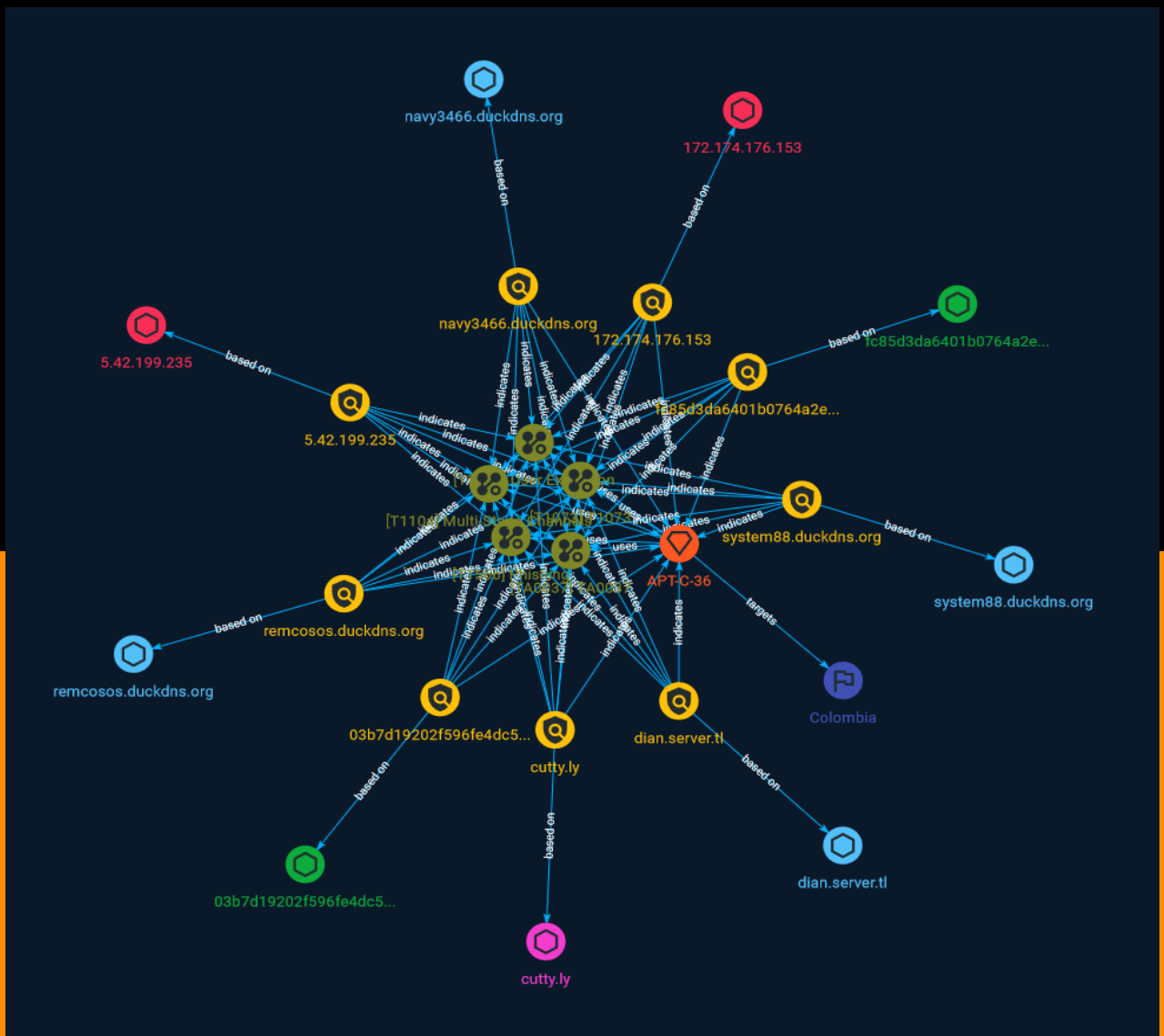

Table of contents

Overview

Entities

Observables

External References

Overview

Description

APT-C-36 (Blind Eagle) is an APT organization suspected to be from South America. Its main targets are located in Colombia, as well as other countries and regions in South America, such as Ecuador and Panama. Since its discovery in 2018, the group has continued to launch attacks against Colombia. Even though security vendors have successively captured and disclosed their attack activities in the past two years, they have not stopped APT-C-36's actions and lurking, and its attacks have become more and more intense.

Confidence

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

15 / 100

Attack-Pattern

Name
Phishing
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

User Execution

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)

Name

TA0037

ID

TA0037

Name

Multi-Stage Channels

ID

T1104

Description

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

Name

T1073

ID

T1073

Indicator

Name
system88.duckdns.org
Pattern Type
stix
Pattern
[hostname:value = 'system88.duckdns.org']
Name
remcosos.duckdns.org
Pattern Type
stix
Pattern
[hostname:value = 'remcosos.duckdns.org']
Name
172.174.176.153

Description

CC=US ASN=AS8075 MICROSOFT-CORP-MSN-AS-BLOCK

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.174.176.153']

Name

cutty.ly

Pattern Type

stix

Pattern

[domain-name:value = 'cutty.ly']

Name

5.42.199.235

Description

ISP: IT Resheniya LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **21:** ``` 220 FTP Server ready. 530 Login incorrect. 214-The following commands are recognized (* =>'s unimplemented): CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV EPRT EPSV ALLO* RNFR RNTO DELE MDTM RMD XRMD MKD XMKD PWD XPWD SIZE SYST HELP NOOP FEAT OPTS AUTH CCC* CONF* ENC* MIC* PBSZ PROT TYPE STRU MODE RETR STOR STOU APPE REST ABOR

USER PASS ACCT* REIN* LIST NLST STAT SITE MLSD MLST 214 Direct comments to root@localhost 211-Features: LANG ru-RU;ko-KR;ja-JP;it-IT;fr-FR;es-ES;en-US;bg-BG;zh-TW;zh-CN MDTM SSCN TVFS MFMT SIZE PROT CCC PBSZ AUTH TLS MFF modify;UNIX.group;UNIX.mode; REST STREAM MLST modify*;perm*;size*;type*;unique*;UNIX.group*;UNIX.mode*;UNIX.owner*; UTF8 EPRT EPSV 211 End ``` ---------- **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDdDMjD9GAZ/yLEl+ig3TcyzKGdB3dl24U/cOEzjexaEcUc MFrjrWktyVAHAGvTuWSHhPU2dfwrfvupXtlW/WJyPkhaS+I6VZtWOnkU0jgyCoh53kaOp45E3tzV ESLedbFYCmQG1o9OiUsl9fS0wpuf4dRvY/WZXKwnOwgiZreh4PZJf8VomfGPhRsk0jNmYKpD4iL6 V+EVeFvQQfIDhkxpWpixnOwnvKE9iRZTDR34m7Ls3DxaYk5GoP9jFXleWZitIYfDXFFkTox6DZtk CyB3g6ibo/CVSeOVqcjJqBzX+jrG26mUZ38CbYCisDWebGEIE+bLaXnx15VbCYCMWMEp Fingerprint: b1:5a:bc:7d:69:4e:62:3d:8e:8c:ff:0f:ce:56:71:42 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa 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 aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc 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 ``` ---------- **25:** ``` 220 mr-1.example.com ESMTP Exim 4.96 Sat, 28 Jan 2023 04:52:48 +0300 250-mr-1.example.com Hello 224.183.40.135 [224.183.40.135] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPECONNECT 250-AUTH PLAIN LOGIN CRAM-MD5 250-CHUNKING 250-STARTTLS 250 HELP ``` ---------- **53:** ``` 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 Resolver name: mr-1.example.com ``` ---------- **80:** ``` HTTP/1.1 403 Forbidden Server: nginx/1.20.2 Date: Tue, 07 Feb 2023 14:09:48 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: keep-alive ``` ---------- **110:** ``` +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE STLS USER SASL PLAIN LOGIN DIGEST-MD5 CRAM-MD5 . ``` ---------- **143:** ``` * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS AUTH=PLAIN AUTH=LOGIN AUTH=DIGEST-MD5 AUTH=CRAM-MD5] Dovecot ready. * CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS AUTH=PLAIN AUTH=LOGIN AUTH=DIGEST-MD5 AUTH=CRAM-MD5 A001 OK Pre-login capabilities listed, post-login capabilities have more. * ID ("name" "Dovecot") A002 OK ID completed. A003 BAD Error in IMAP command received by server. * BYE Logging out A004 OK Logout completed. ``` ---------- **443:** ``` HTTP/1.1 403 Forbidden Server: nginx/1.20.2 Date: Sat, 04 Feb 2023 12:32:11 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: keep-alive ``` HEARTBLEED: 2023/02/04 12:32:31 5.42.199.235:443 - SAFE ---------- **465:** ``` 220 mr-1.example.com ESMTP Exim 4.96 Sun, 15 Jan 2023 01:28:22 +0300 250-mr-1.example.com Hello 224.69.149.86 [224.69.149.86] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPECONNECT 250-AUTH PLAIN LOGIN

CRAM-MD5 250-CHUNKING 250 HELP ``` HEARTBLEED: 2023/01/14 22:28:29 5.42.199.235:465 - SAFE ---------- **587:** ``` 220 mr-1.example.com ESMTP Exim 4.96 Wed, 18 Jan 2023 09:14:01 +0300 250-mr-1.example.com Hello 224.228.17.197 [224.228.17.197] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPECONNECT 250-AUTH PLAIN LOGIN CRAM-MD5 250-CHUNKING 250-STARTTLS 250 HELP ``` ---------- **995:** ``` +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE USER SASL PLAIN LOGIN DIGEST-MD5 CRAM-MD5 . ``` ---------- **1500:** ``` HTTP/1.1 301 Moved Permanently Content-Length: 0 Connection: close Location: https://5.42.199.235/ Date: Mon, 30 Jan 2023 15:59:17 GMT ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.42.199.235']

Name

fc85d3da6401b0764a2e8a5f55334a7d683ec20fb8210213feb6148f02a30554

Description

multiple_versions SHA256 of e4d2799f3001a531d15939b1898399b4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fc85d3da6401b0764a2e8a5f55334a7d683ec20fb8210213feb6148f02a30554']

Name

03b7d19202f596fe4dc556b7da818f0f76195912e29d728b14863dda7b91d9b5

Description

Win.Packed.Trojanx-9818175-0 SHA256 of 07af8778de9f2bc53899aac7ad671a72

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '03b7d19202f596fe4dc556b7da818f0f76195912e29d728b14863dda7b91d9b5']

Name

navy3466.duckdns.org

Pattern Type

stix

Pattern

[hostname:value = 'navy3466.duckdns.org']

Name

dian.server.tl

Pattern Type

stix

Pattern
[hostname:value = 'dian.server.tl']

Intrusion-Set

Name
APT-C-36

Description
[APT-C-36](https://attack.mitre.org/groups/G0099) is a suspected South America espionage group that has been active since at least 2018. The group mainly targets Colombian government institutions as well as important corporations in the financial sector, petroleum industry, and professional manufacturing.(Citation: QiAnXin APT-C-36 Feb2019)

Country

Name
Colombia

Domain-Name

Value
cutty.ly

StixFile

Value
fc85d3da6401b0764a2e8a5f55334a7d683ec20fb8210213feb6148f02a30554
03b7d19202f596fe4dc556b7da818f0f76195912e29d728b14863dda7b91d9b5

Hostname

Value
navy3466.duckdns.org
system88.duckdns.org
remcosos.duckdns.org
dian.server.tl

IPv4-Addr

Value
5.42.199.235
172.174.176.153

External References

- https://otx.alienvault.com/pulse/64419d343c9d98fc279185f7
- https://mp-weixin-qq-com.translate.goog/s?__biz=MzUyMjk4NzExMA%3D%3D&mid=2247492492&idx=1&sn=5cfd1606d6a3349c8cf0d8e1edba5c84&chksm=f9c