

# The ATT&CK Latin American APT Playbook


MITRE  
**ATT&CKCON 3.0**

The MITRE | ATT&CK<sup>®</sup> Conference

**kaspersky**




**Santiago Pontiroli**

 @spontiroli  
Argentina



**Dmitry Bestuzhev**

 @dimitribest  
USA



---

Not all TTPs are created equal

3

Since the threat actors' origin, culture, and language is often different, it's not uncommon for tactics, techniques, and procedures (TTPs) to present marked differences between regions.

---

Can we adopt and align to the MITRE ATT&CK Framework to profile **regional threat actors**? What are the nuances of such a process?

---

Understanding the **context** of each threat actor and their operations highlights the **importance of being able to map to ATT&CK from both finished reporting and raw data.**



## Machete aka Ragua aka "Arkantos Live Control" (APT C-43)

4

REPÚBLICA BOLIVARIANA DE VENEZUELA MINISTERIO DEL PODER POPULAR PARA LA DEFENSA COMANDO ESTRATÉGICO OPERACIONAL REGIÓN ESTRATÉGICA DE DEFENSA INTEGRAL LOS ANDES ZONA OPERATIVA DE DEFENSA INTEGRAL TRUJILLO				CLASIFICACIÓN DE SEGURIDAD  CONFIDENCIAL	
FORMA DE MENSAJE					
ESPACIO PARA EL USO DEL CENTRO DE COMUNICACIONES					
PRECEDENCIA: IMPORTANTE	TIPO DE MENSAJE		SÍMBOLO CONTABLE	ORIGINAL O REFIERASE A	CLASIFICACIÓN DE REFERENCIA
ACCIÓN:	IND	MUL	SIM	RAD. 0268 DE FECHA 24MAY19 DE LA RED1 LOS ANDES	CONFIDENCIAL
URGENTE		X		OPERACIONES	
DE:	G/D. CMDTE DE LA ZODI N° 23 TRUJILLO.				
PARA:	G/B. CMDTE DEL CZGNB N° 23 TRUJILLO; G/B. DIR. MILICIA ZODI TRUJILLO; CNEL. CMDTE. DEL REG. GUARDIA DEL PUEBLO; TCNEL. CMDTE 222 B.I.M. RIVAS DÁVILA; TCNEL. CMDTE. DEL GAES TRUJILLO; MY. CMDTE. U.R.I.A. TRUJILLO; CNEL. DIR. CIRMI TRUJILLO; CNEL. DIR. INCES MILITAR; CNEL. DIR. INSTRUCCIÓN PRE MILITAR, C.C. E.S.G.C.L.C; CAP. E.V.C.L.C; MY. DIR. ESTACIÓN DE METEOROLOGÍA; MY. DIR. DGCIM TRUJILLO; C.C. DIR. P.E.M. IPSFA TRUJILLO; ITTE. OFICIAL FUERZA DE CHOQUE TRUJILLO.				
RADIOGRAMA N° 0 1204					
PACOFI, INFORMOLE, GRUPOS DE EXTREMA DERECHA PRETENDEN LLEVAR A CABO ACCIONES TALES COMO ASALTOS, ACTOS DE SABOTAJE, CAPTACIÓN DE EFECTIVOS, ENTRE OTRAS; EN CONTRA DE UNIDADES, DEPENDENCIAS O INSTITUTOS EDUCATIVOS DE LA FANB, EMPLEANDO PARA ELLOS MERCENARIOS PORTANDO UNIFORMES MILITARES O POLICIALES; EN TAL SENTIDO SE ORDENA DAR Estricto CUMPLIMIENTO A LAS SIGUIENTES ORDENES:					
<ol style="list-style-type: none"><li>1. EXTREMAR LAS MEDIDAS DE SEGURIDAD DE LAS INSTALACIONES CON ESPECIAL ÉNFASIS EN ARMAMENTO, MUNICIONES, MATERIALES Y EQUIPOS ASIGNADOS.</li><li>2. NINGUNA UNIDAD O DEPENDENCIA DEBE MOVILIZAR PERSONAL O VEHÍCULOS SIN AUTORIZACIÓN DE SU COMANDO SUPERIOR</li><li>3. REPORTAR DE INMEDIATO CUALQUIER NOVEDAD O ACTIVIDAD SOSPECHOSA</li></ol>					
INSTRUCCIONES ESPECIALES				DIA: 31 MES: 05	HORA: 18:00 AÑO: 2019
REDACTOR	SÍMBOLO: PERSONAL		NOMBRE Y CARGO:		
	NOMBRE Y CARGO:				
	CNEL. YSMAEL ROMAY OPERACIONES 2019 TRUJILLO		JOSE GREGORIO LAYA PEREZ GENERAL DE DIVISIÓN CMDTE DE LA ZODI N° 23 (TRUJILLO)		
	TEL.F. 0424-8010967 PAS. N° 1 N° DESPACHO				
CLASIFICACIÓN DE SEGURIDAD					
CONFIDENCIAL					
¡CHAVEZ VIVE... LA PATRIA SIGUE!					

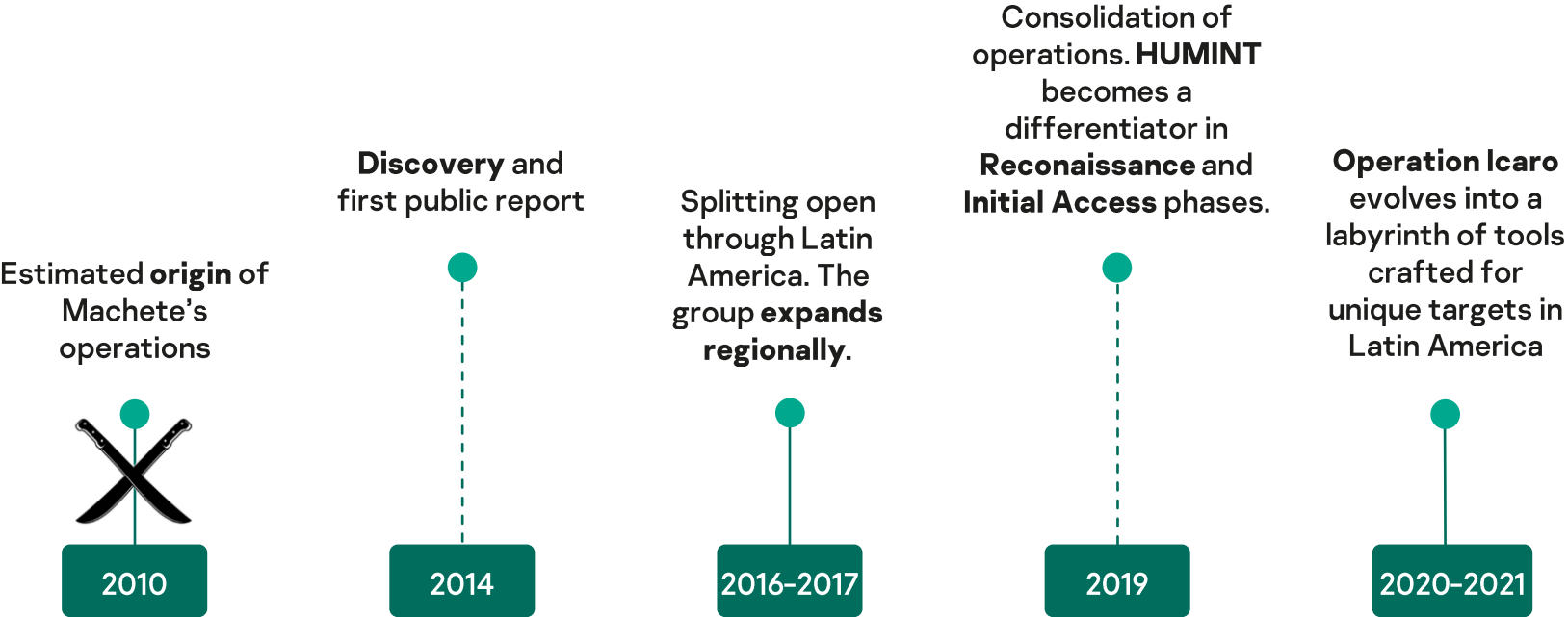
### Victimology

Primarily focuses its operations within Latin America, emphasizing Venezuela, but also in the US, Europe, Russia, and parts of Asia. **Since 2010**, this list has expanded according to Machete's goals.

**Using social-engineering and spear-phishing** to target intelligence services, embassies, armed forces, and other key strategic objectives.

Operators have extensive knowledge on how and when to approach their victims, designing custom decoy documents of interest to government or military entities.

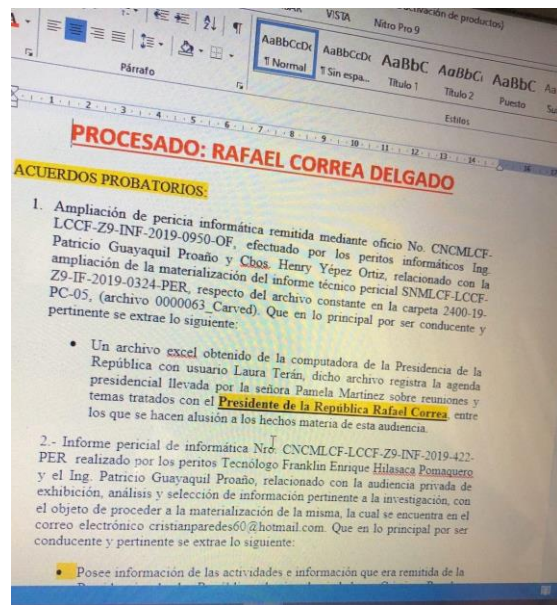
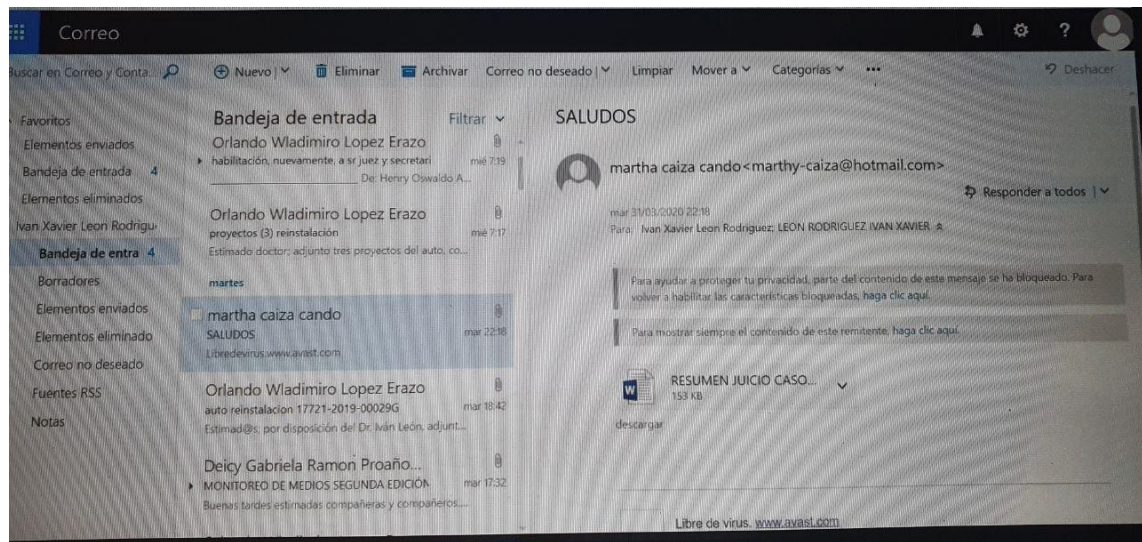
# Timeline of Machete





# Timeline of Machete – COVID-19 Operation

6



```
152
153 <script>
154 document.write("Usuarios Online: " + Math.floor((Math.random() * 99999) + 9000));
155 </script>Usuarios Online: 79303
156
```

# Machete's TTPs

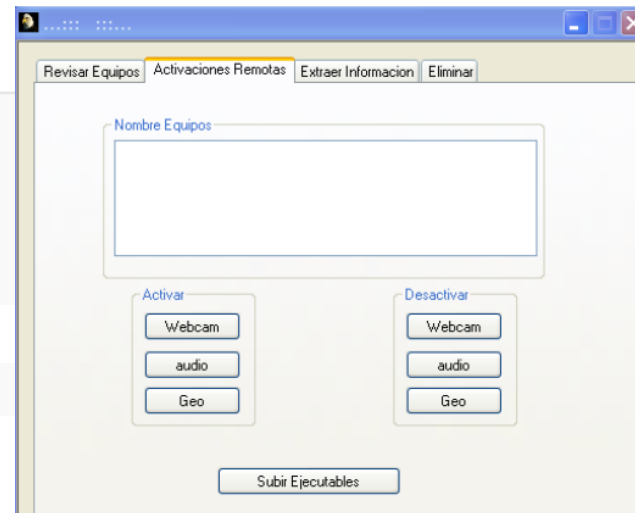
7

<b>Initial access</b>	T1189 – Drive-by Compromise T1566.001 – Spear phishing attachment T1566.002 – Spear phishing link
<b>Execution</b>	T1059.006 – Python T1059.005 – Visual Basic T1059.003 – Windows Command Shell T1053.005 – Scheduled Tasks T1204.002 – Malicious File T1204.001 – Malicious Link
<b>Persistence</b>	T1053.005 – Scheduled Tasks
<b>Privilege Escalation</b>	T1053.005 – Scheduled Tasks
<b>Defense Evasion</b>	T1036.005 – Match Legitimate name or location T1218.007 – Msiexec T1221 – Template Injection (pptx)

<b>Credential Access</b>	T1056.001 – Keylogging T1555.003 – Credentials from Web Browsers
--------------------------	---

<b>Collection</b>	T1052.001 – Exfiltration over USB (copies files to a special USB device if inserted) T1005 – Data from Local System (capture geolocation data) T1123 – Audio Capture T1115 – Clipboard data T1056.001 – Keylogging T1113 – Screen Capture T1125 – Video Capture
-------------------	---

<b>Exfiltration</b>	T1048.003 – Exfiltration over Unencrypted/Obfuscated Non-C2 Protocol (FTP)
---------------------	--



---

## Blind Eagle (APT C-36)

8



---

Using Spanish language in their spear-phishing emails targeting Colombia, Ecuador, Spain, and Panama.

---

Remote Access Tools Trojans (RATs), such as njRAT, LimeRAT, Imminent Monitor, and others.

---

**Multi-stage and encrypted payload**, process injection, DLL sideloading, using packers and obfuscation techniques common to Agent Tesla and similar .NET information stealers.



# Blind Eagle APT C-36 TTPs

<b>Reconnaissance</b>	T1598: Phishing for Information	<b>Defense Evasion</b>	T1548: Abuse Elevation Control Mechanism T1140: Deobfuscate/Decode Files or Information T1564: Hide Artifacts
<b>Resource Development</b>	T1583: Acquire Infrastructure T1584: Compromise Infrastructure T1588: Obtain Capabilities	<b>Credential Access</b>	T1555: Credentials from Password Stores T1056: Input Capture
<b>Initial Access</b>	T1566: Phishing	<b>Discovery</b>	*
<b>Execution</b>	T1059: Command and Scripting Interpreter T1106: Native API T1053: Scheduled Task/Job T1204: User Execution	<b>Collection</b>	T1560: Archive Collected Data T1123: Audio Capture T1119: Automated Collection T1115: Clipboard Data T1005: Data from Local System T1056: Input Capture T1113: Screen Capture T1125: Video Capture
<b>Persistence</b>	T1547: Boot or Logon Autostart Execution	<b>Command and Control</b>	T1071: Application Layer Protocol T1132: Data Encoding T1219: Remote Access Software
<b>Privilege Escalation</b>	T1548: Abuse Elevation Control Mechanism T1547: Boot or Logon Autostart Execution	<b>Exfiltration</b>	T1041: Exfiltration Over C2 Channel

# Espionage or just business?

The Puppeteer Group is an international cyberespionage mercenary group with its roots in Latin America. They have no allegiance and work for the highest bidder.



---

A well-organized gang of digital **mercenaries**, targeting governments, politicians, and journalists all over Latin America.

---

The Puppeteer's are master manipulators. They draw the strings to manipulate each of their targets, **leveraging different information they've stolen to gain the interest of their new targets.**

---

Their targets are journalists, opposition media, and politicians.



Estocolmo, 1 de noviembre de 2014

Señor Economista  
Rafael Correa Delgado  
Presidente Constitucional de la República  
En su despacho.-

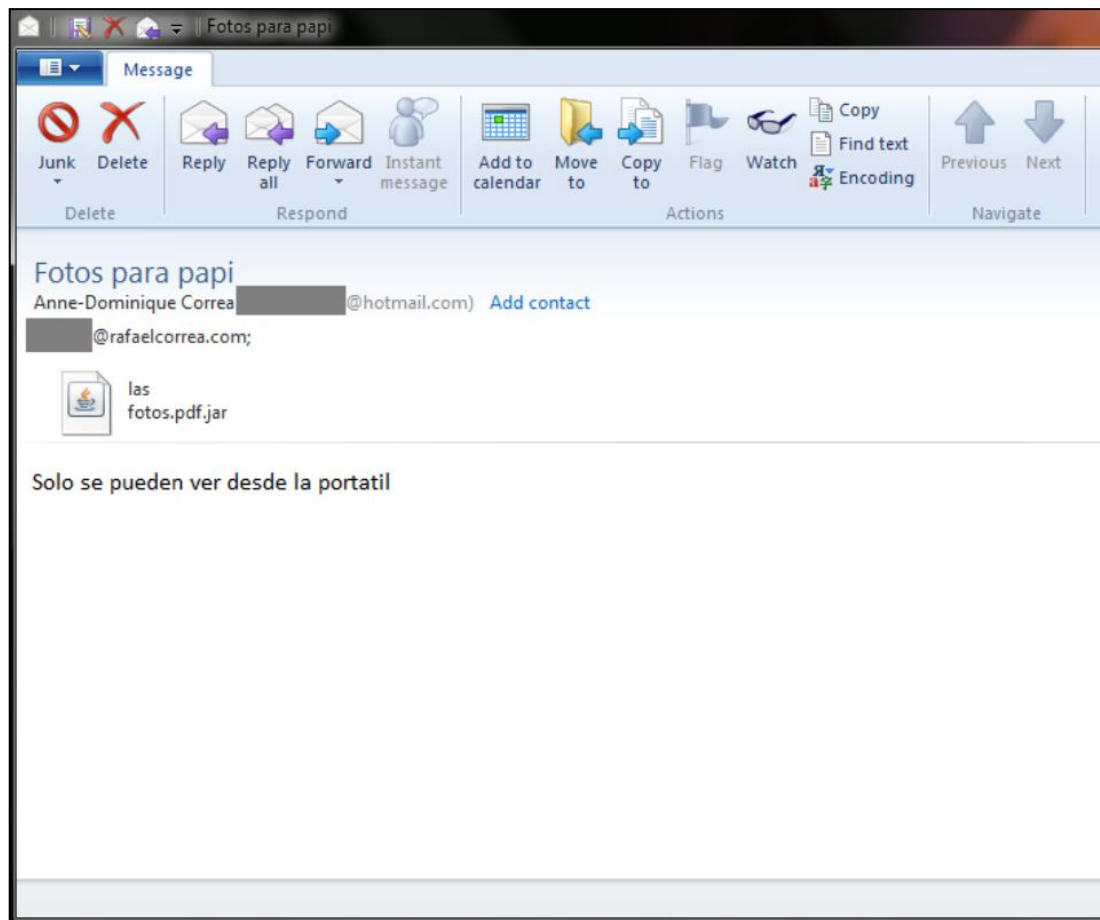
Señor Presidente:

En atención a su pedido, sírvase encontrar en calidad de anexo a la presente comunicación, un informe sucinto sobre el proyecto "Gripen Ecuador".

Cumpliré con la mayor celeridad sus instrucciones de reactivación del proyecto, efecto para el que debo contar con el contingente del Ministerio de Defensa Nacional.

Reitero a usted señor Presidente mis sentimientos de consideración distinguida,

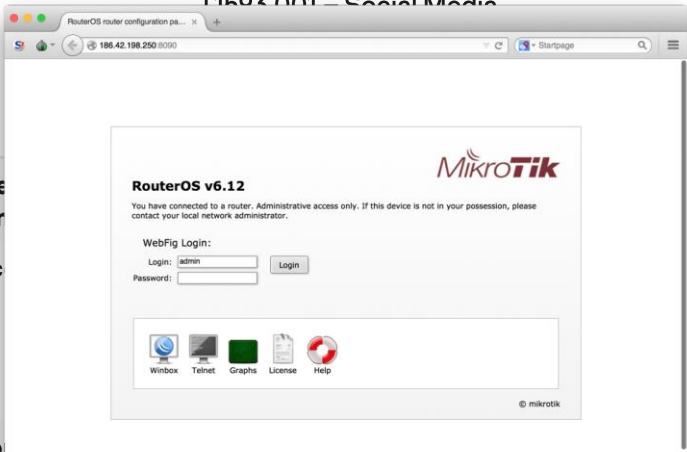
Muy atentamente,



Puppeteers' TTPs

Reconnaissance

- T1598.002 – Spear Phishing Attachment
- T1593.002 – Search Engines
- T1593.001 – Social Media



Resource  
Develop  
Initial Ac

Execution

- T1203 – Exploitation for Client Execution

Persistence

- T1547.001 – Registry Run Key / Startup Folder
- T1037.005 – Startup Items
- T1574.010 – Services File Permissions Weakness

Privilege Escalation

- T1547.001 – Registry Run Key / Startup Folder
- T1037.005 – Startup Items
- T1574.010 – Services File Permissions Weakness
- T1055.012 – Process Hollowing

Defense Evasion

- T1574.010 – Services File Permissions Weakness
- T1070.004 – File Deletion



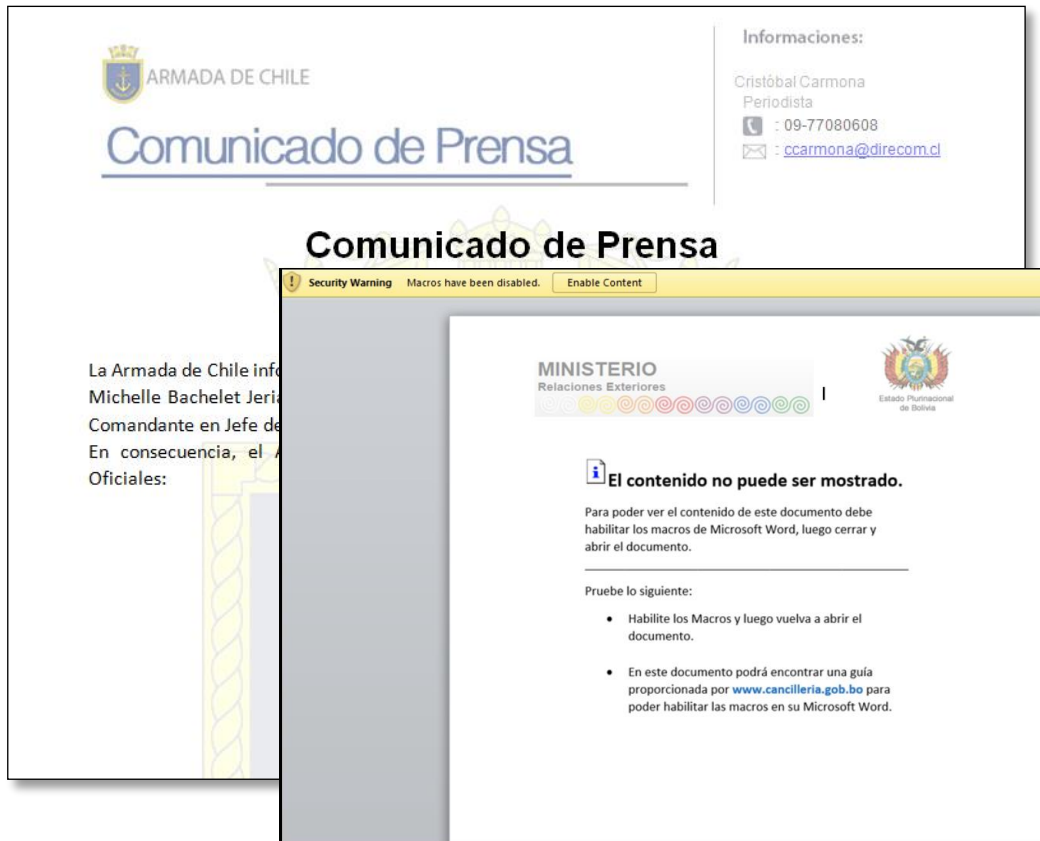
Command and Control

- T1071.004 – DNS
- T1573.001 – Symmetric Cryptography
- T1105 – Ingress Tool Transfer
- T1090.003 – Multi-hop Proxy

Exfiltration

- T1567.002 – Exfiltration to Cloud Storage

ision  
g  
Web  
discovery



Government and military institutions from Chile targeted by a multi-stage malware attack deployed by an unknown actor.

Using malicious documents with embedded macros that leverage **PowerShell scripts generated by offensive security frameworks like Veil and PowerShell Empire.**

The primary target for this campaign was a systems developer company used by the Ministry of Defense of Chile.



---

## Pisco Gone Sour's TTPs

14

<b>Reconnaissance</b>	T1597.001 – Threat Intel Vendors
<b>Resource Development</b>	T1586.002 – Email Accounts T1587.001 – Malware T1585.002 – Email Accounts T1588.001 – Malware T1588.002 – Tool
<b>Initial Access</b>	T1566.001 – Spear Phishing Attachment T1199 – Trusted Relationship
<b>Execution</b>	T1059.001 – PowerShell T1059.006 – Python T1059.005 – Visual Basic
<b>Credential Access</b>	T1555.003 – Credentials from Web Browsers T1606.001 – Keylogging
<b>Collection</b>	T1560.003 – Archive via Custom Method T1185 – Browser Session Hijack T1056.001 – Keylogging
<b>Command and Control</b>	T1071.001 – Web Protocols
<b>Exfiltration</b>	T1567.002 – Exfiltration to Cloud Storage

**Initial Access Brokers**  
gain their foothold into  
the victim's network and  
then resell it to other  
cybercriminals.

# A custom-tailored malware implants boutique

---

Targeting Portuguese speaking entities, using digitally signed malware, satellite uplinks, and extensive tools for data gathering.

---

Masquerading as a security company, Poseidon used harvested secrets to blackmail targets.

---

Volatile infrastructure, discarded after each operation.

---

As with Puppeteer, Poseidon is not a state-sponsored attack but rather a commercial threat player



## Poseidon's TTPs

17

<b>Reconnaissance</b>	T1592: Gather Victim Host Information T1589: Gather Victim Identity Information T1590: Gather Victim Network Information T1591: Gather Victim Org Information T1598: Phishing for Information	<b>Collection</b>	T1560: Archive Collected Data T1119: Automated Collection T1005: Data from Local System T1039: Data from Network Shared Drive T1025: Data from Removable Media
<b>Resource Development</b>	T1583: Acquire Infrastructure T1586: Compromise Accounts T1587: Develop Capabilities T1585: Establish Accounts T1588: Obtain Capabilities T1608: Stage Capabilities	<b>Discovery</b>	T1087: Account Discovery T1135: Network Share Discovery T1057: Process Discovery T1518: Software Discovery T1082: System Information Discovery T1016: System Network Configuration Discovery
<b>Initial Access</b>	T1566: Phishing T1078: Valid Accounts	<b>Credential Access</b>	T1003: OS Credential Dumping
<b>Execution</b>	T1059: Command and Scripting Interpreter T1204: User Execution	<b>Defense Evasion</b>	T1564: Hide Artifacts
<b>Persistence</b>	T1037: Boot or Logon Initialization Scripts	<b>Command and Control</b>	T1071: Application Layer Protocol T1090: Proxy
<b>Privilege Escalation</b>	T1037: Boot or Logon Initialization Scripts	<b>Exfiltration</b>	T1020: Automated Exfiltration T1041: Exfiltration Over C2 Channel

---

## Saguaro – the initial access group

---

Initial infection vector:

Social engineering (email)

---

**Targets:** A cyberespionage campaign targeting healthcare and financial organizations, research institutions, universities, internet providers, and PR agencies in Latin America since 2009. The Spanish-speaking attackers behind the campaign use a spear-phishing email to infect devices with malware capable of spying on the victims and collecting confidential information.

# SAGUARO



FIRST KNOWN SAMPLE

2009

DISCOVERY

2009

NUMBER OF TARGETS

10000-300000

CURRENT STATUS

Active

TOP TARGETED COUNTRIES

Mexico





---

## Saguaro's TTPs

19

<b>Reconnaissance</b>	T1589.002 – Email addresses
<b>Initial Access</b>	T1566.001 – Spear phishing Attachment
<b>Execution</b>	T1204.002 – Malicious File
<b>Persistence</b>	T1547.015 – Login Items
<b>Privilege Escalation</b>	T1547.015 – Login Items T1055.013 – Process Doppelganging
<b>Defense Evasion</b>	T1055.013 – Process Doppelganging T1553.002 – Code Signing T1497.001 – System Checks
<b>Credential Access</b>	T1555.003 – Credentials from Web Browsers T1555.005 – Password Managers RDP credentials, BTC
<b>Discovery</b>	T1082 – System Information Discovery T1497.001 – System Checks
<b>Collection</b>	T1005 – Data from Local Systems T1114.001 – Local Email Collection
<b>Command and Control</b>	T1219 – Remote Access Software
<b>Exfiltration</b>	T1567.002 – Exfiltration to Cloud Storage

---

## Global Threat Actors operating in Latin America

20



---

If it looks like a duck, swims like a duck, and quacks like a duck, then it probably is a financially motivated threat actor operating in Latin America.

---

It's unusual for regional actors to target entities outside Latin America. However, **global actors run their campaigns locally and adapt their TTPs.**

---

The combination of cyber-espionage, mercenary groups, and financially motivated actors makes it **difficult to cluster and correlate an operation with a particular group.**

# Never a dull moment with APT-38

Also known as HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY, APT38, Stardust Chollima, BeagleBoyz, NICKEL GLADSTONE, Gods Apostles, Gods Disciples, ZINC, Whois Team. And now... The Artist, formerly known as Prince?

---

Latin American banking institutions became their target of choice during 2019. In particular multibank ATM networks and payment processors.

---

Different tooling but similar TTPs to other campaigns. Extensive **Reconnaissance** phase and careful choice of initial targets.

---

.NET downloader and a multi-stage PowerShell malware, loading from memory.




## Lazarus' TTPs

22

<b>Reconnaissance</b>	T1589: Gather Victim Identity Information T1591: Gather Victim Org Information	<b>Defense Evasion</b>	T1548: Abuse Elevation Control Mechanism T1140: Deobfuscate/Decode Files or Information
<b>Resource Development</b>	T1583: Acquire Infrastructure T1587: Develop Capabilities T1585: Establish Accounts T1588: Obtain Capabilities	<b>Credential Access</b>	T1056: Input Capture
<b>Initial Access</b>	T1566: Phishing	<b>Discovery</b>	*
<b>Execution</b>	T1059: Command and Scripting Interpreter T1204: User Execution T1047: Windows Management Instrumentation	<b>Collection</b>	T1005: Data from Local System T1039: Data from Network Shared Drive T1025: Data from Removable Media T1056: Input Capture
<b>Persistence</b>	T1543: Create or Modify System Process	<b>Command and Control</b>	T1071: Application Layer Protocol
<b>Privilege Escalation</b>	T1548: Abuse Elevation Control Mechanism T1543: Create or Modify System Process	<b>Exfiltration</b>	T1020: Automated Exfiltration T1041: Exfiltration Over C2 Channel

Global Processing Center,LTD



First Name:

Last Name:

Gender: ☒ M ☐ F

Age:

Contact Mail:

Phone:

```
$pass = "PowershellAgent"
$st="PowershellAgent"
$it="PowershellAgent"
$ps_content="oMhkxcU6XSD6HFDrpso602UqOTbe7wuP8NbmFI+D1ruTluOJvchI2qwD+Vb"
function crypt_do {
    Param (
        $crypted
    )
    if($crypted -is [string]){
        $crypted = [Convert]::FromBase64String($crypted)
    }

    $r = new-Object System.Security.Cryptography.RijndaelManaged
    $pass = [System.Text.Encoding]::UTF8.GetBytes($pass)
    $st = [System.Text.Encoding]::UTF8.GetBytes($st)

    $r.Key = (new-Object Security.Cryptography.PasswordDeriveBytes $pass,
    $r.IV = (new-Object Security.Cryptography.SHA1Managed).ComputeHash(

    $d = $r.CreateDecryptor()
    $ms = new-Object IO.MemoryStream @($crypted)
    $cs = new-Object Security.Cryptography.CryptoStream $ms,$d,"Read"
    $sr = new-Object IO.StreamReader $cs
```



# Living off the land as an APT

---

Extensive usage of LOLBins (for Living Off the Land Binaries) such as **msiexec.exe**, **mshta.exe**, **rundll32.exe**, and **powershell.exe**.

---

Persistence depends on the victim.



---

Multi-stage, obfuscated, malware. Usually **digitally** signed.

---

Infamous for their **CLOP** ransomware and companion **CLoP^LEAKS** website

## TA505's TTPs

25

<b>Reconnaissance</b>	T1589: Gather Victim Identity Information T1591: Gather Victim Org Information T1598: Phishing for Information	<b>Defense Evasion</b>	T1564: Hide Artifacts
<b>Resource Development</b>	T1583: Acquire Infrastructure T1586: Compromise Accounts T1587: Develop Capabilities T1585: Establish Accounts T1588: Obtain Capabilities T1608: Stage Capabilities	<b>Collection</b>	T1119: Automated Collection T1115: Clipboard Data T1005: Data from Local System T1039: Data from Network Shared Drive T1025: Data from Removable Media T1114: Email Collection T1056: Input Capture
<b>Initial Access</b>	T1078: Valid Accounts	<b>Discovery</b>	T1087: Account Discovery
<b>Execution</b>	T1059: Command and Scripting Interpreter T1106: Native API T1204: User Execution	<b>Credential Access</b>	T1555: Credentials from Password Stores, T1212: Exploitation for Credential Access, T1056: Input Capture
<b>Persistence</b>	T1547: Boot or Logon Autostart Execution	<b>Command and Control</b>	T1071: Application Layer Protocol T1568: Dynamic Resolution T1008: Fallback Channels T1105: Ingress Tool Transfer T1219: Remote Access Software
<b>Privilege Escalation</b>	T1547: Boot or Logon Autostart Execution	<b>Exfiltration</b>	T1020: Automated Exfiltration T1041: Exfiltration Over C2 Channel
		<b>Impact</b>	T1486: Data Encrypted for Impact T1490: Inhibit System Recovery

# LOLBAS

☆ Star 4,128



## Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

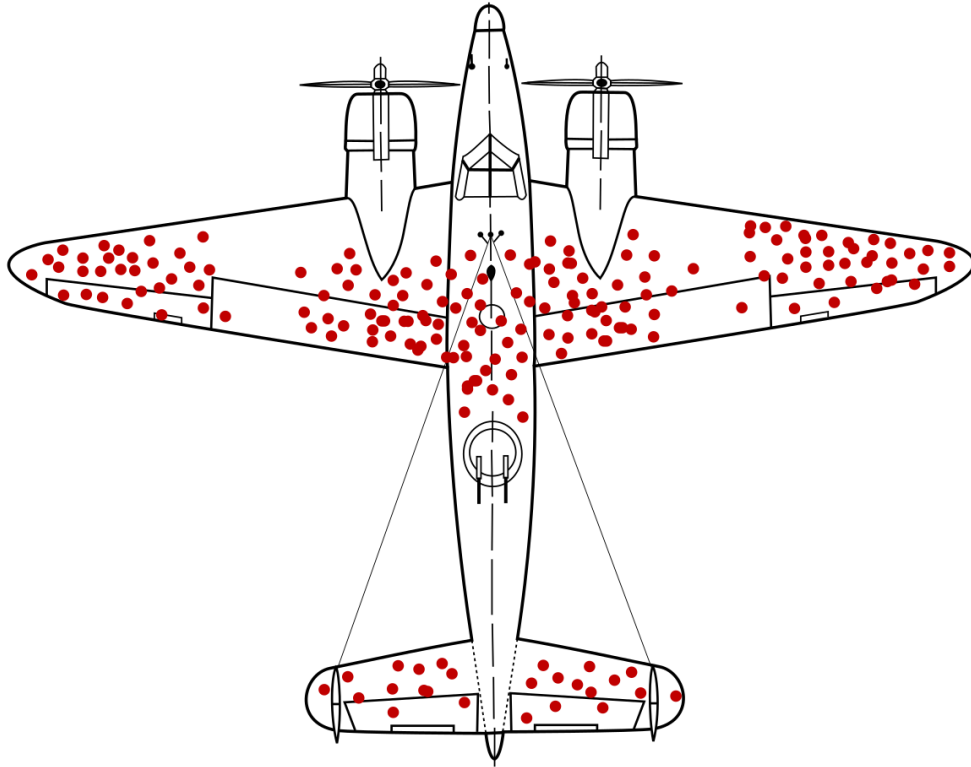
If you want to contribute, check out our [contribution guide](#). Our [criteria list](#) sets out what we define as a LOLBin/Script/Lib.

*MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation.* You can see the current ATT&CK® mapping of this project on the [ATT&CK® Navigator](#).

If you are looking for UNIX binaries, please visit [gtfobins.github.io](#).

Search among 156 binaries by name (e.g. 'MSBuild'), function (e.g. 'execute'), type (e.g. '#Script') or ATT&CK info (e.g. 'T1218')

Binary	Functions	Type	ATT&CK® Techniques
<a href="#">AppInstaller.exe</a>	<a href="#">Download</a>	Binaries	<a href="#">T1105: Ingress Tool Transfer</a>
<a href="#">AspNet_Compiler.exe</a>	<a href="#">AWL bypass</a>	Binaries	<a href="#">T1127: Trusted Developer Utilities Proxy Execution</a>
<a href="#">At.exe</a>	<a href="#">Execute</a>	Binaries	<a href="#">T1053.002: At (Windows)</a>
<a href="#">Atbroker.exe</a>	<a href="#">Execute</a>	Binaries	<a href="#">T1218: Signed Binary Proxy Execution</a>
<a href="#">Bash.exe</a>	<a href="#">Execute</a> <a href="#">AWL bypass</a>	Binaries	<a href="#">T1202: Indirect Command Execution</a>



Survivorship bias is the logical error of concentrating on the people or things that made it past some selection process and overlooking those that did not, typically because of their lack of **visibility**.

The gambler's fallacy, also known as the Monte Carlo fallacy, is the incorrect belief that, if a particular event occurs more frequently than normal during the past, it is less likely to happen in the future (or vice versa).

---

Things, which didn't fit in this presentation

28

**Satellite Turla**

**Dark Tequila Añejo**

**xPan** – father of Hospitals  
targeting Ransomware





---

**“ Tell me what you know, then tell me what you don't know, and only then can you tell me what you think. Always keep those three separated.**

---

*Colin Powell*

# Thank you for your time and attention!



**Santiago Pontiroli**

 @spontiroli

Argentina



**Dmitry Bestuzhev**

 @dimitribest

USA

MITRE  
**ATT&CKCON 3.0**

The MITRE | ATT&CK<sup>®</sup> Conference

**kaspersky**