Malware en LATAM:
La verdad de la milanesa

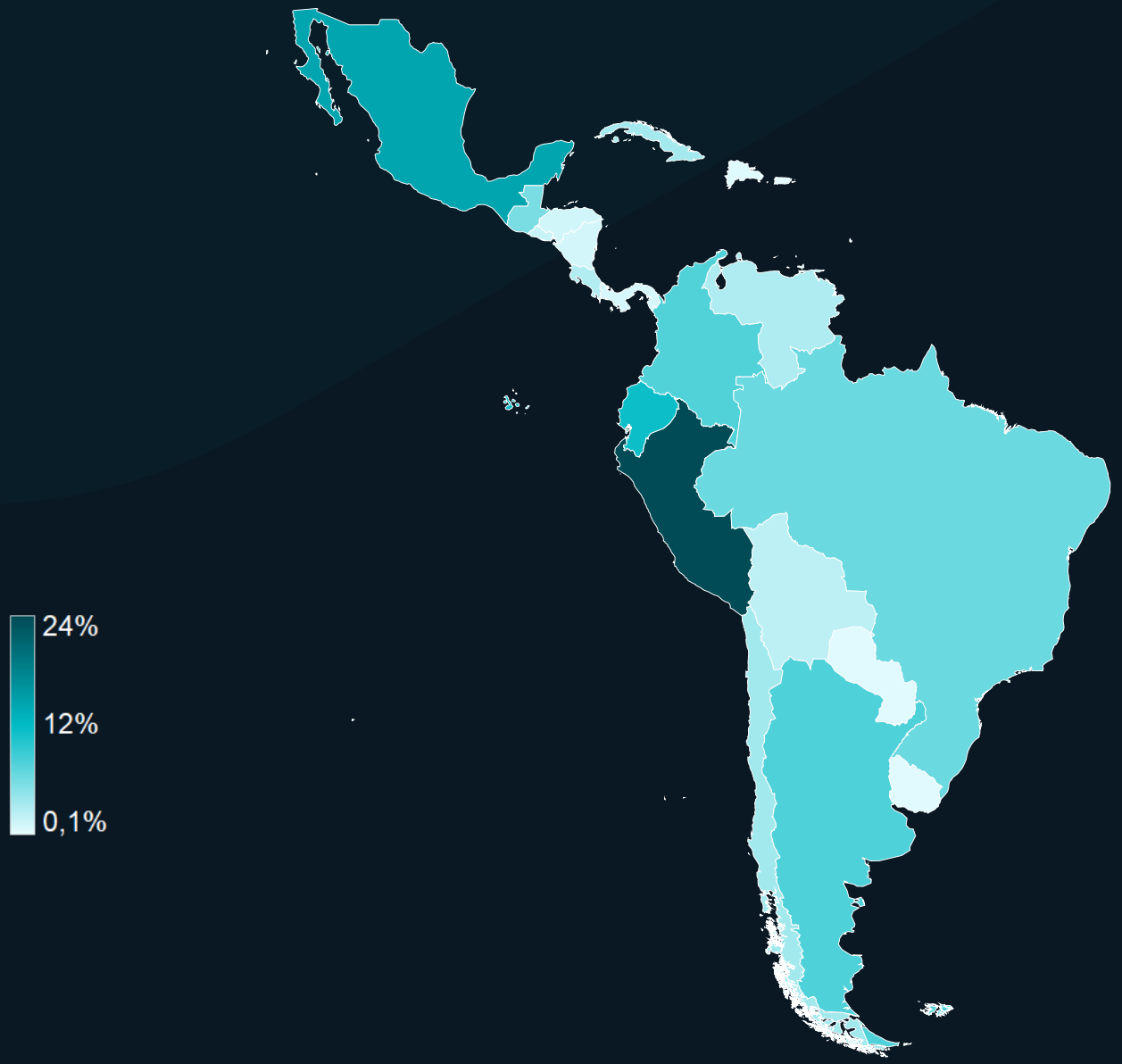
Martina Lopez
Security Researcher @ ESET

- Tipo de archivo
- Tipo de amenaza
- Familia
- Variante
- Extras

PDF/TrojanDropper.Agent.DGT

MSIL/Filecoder.LokiLocker

Win32/Packed.BlackMoon.A

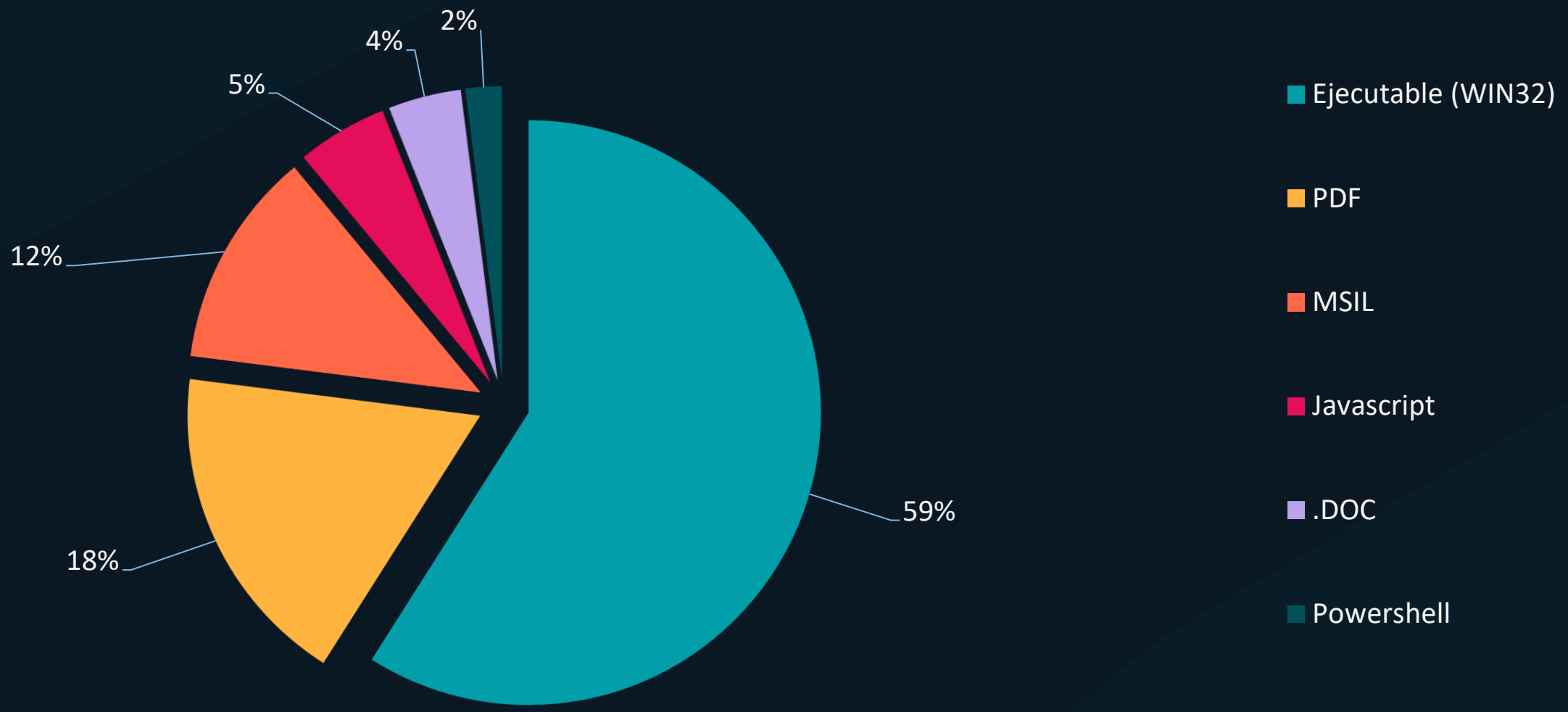


Distribución de detecciones regionales

Familias más detectadas

1. **Ramnit – Botnet & downloader**
2. **Zurgop – Trojan downloader**
3. **Remcos – RAT**
4. **Delf – Trojan downloader**
5. **Phorpiex – Worm**

Filetypes


2%
4%
5%
12%
18%
59%
Ejecutable (WIN32)
PDF
MSIL
Javascript
.DOC
Powershell

Top vulnerabilidades

Nomenclatura	Severidad	Permite	Programa afectado
CVE-2012-0143	9.3/10 - alta	Ejecución de código remoto	Excel 2003 / Office 2008 (Mac)
CVE-2012-0159	9.3/10 - alta	Ejecución de código remoto	Windows XP / Windows 7 / Server 2003 / Server 2008
CVE-2018-8120	7/10 - alta	Escalación de privilegios	Windows 7 / Server 2008

Comportamientos (ft. MITRE ATT&CK)

Acceso Inicial	Ejecución	Evasión de defensas
T1566 – Phishing *Adjuntos y enlaces maliciosos*	T1059 – Command and Scripting Interpeter *Abuso de Powershell o VB para comandos, scripts y binarios*	T1574 – Hijack Execution Flow *Modificar procesos activos*
T1078 – Valid accounts *Abuso de credenciales legítimas robadas o compradas*	T1078 – Software deployment tools *Abuso de software en la red*	T1562 – Impair defenses *Desactivación de mecanismos defensivos*
T1195 – Supply Chain Compromise *Manipulación de productos legítimos a maliciosos*	T1195 – WMI *Administrador nativo para cargas y comandos*	T1195 – Process Injection *Inyección de código en espacios de memoria de procesos activos*

Perú zombie

Paraíso de botnets

VictoryGate: ESET disrumpe botnet utilizada para minar criptomonedas que afecta principalmente a Perú

ESET descubre y disrumpe parte de la operación de VictoryGate, una botnet compuesta principalmente por equipos comprometidos en Perú y que es utilizada para minar criptomonedas.

• 22/4/2020

In 2020, the leader in cryptomining activity per country was Thailand, where ESET telemetry registered 17.9% of all detections. The remaining places in the top three were taken by Latin American countries – Peru with 10.1% of detections and Ecuador with 5.1%.

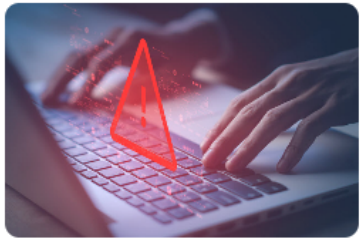
Ecuador, Venezuela y Colombia

Espionaje (y no de película)

Operación Absoluta: espionaje dirigido a empresas y organismos gubernamentales de Colombia

El equipo de investigación de ESET analizó una campaña de espionaje que utiliza el malware AsyncRAT que apunta a organismos gubernamentales y empresas de diversas industrias de Colombia.

• 22/2/2023



Campaña de malware dirigida a Ecuador distribuye el troyano njRAT y utiliza correos falsos de demandas judiciales

Investigadores de ESET analizaron una campaña para espiar y robar información dirigida a empresas privadas, entidades gubernamentales y entidades del sector de salud durante el primer semestre de 2023.

• 26/7/2023

El ABC de los troyanos bancarios

Por y para Latinoamérica

```
lea     edx, [ebp+var_10] ; System::UnicodeString
mov     eax, offset userAgent_enc ; LA CON[illegible] DE TU MADRE
call    decryptString
mov     edx, [ebp+var_10]
lea     eax, [ebx+THttpCli_string_Agent]
call    System_UStrAsg
mov     eax, [ebp+TCustomMemoryStream_Self]
mov     [ebx+THttpCli_TStream_RcvdStream], eax
mov     eax, ebx          ; THttpCli_Self
call    THttpCli_Get
```

Win32/Spy.Lokorrito

¡Gracias!