GESTIÓN DE INCIDENTES DE SEGURIDAD EN LA PROTECCIÓN DE DATOS PERSONALES

Detección de Ransomware con Seguridad Cognitiva

Ph.D(c) Juan Herrera Silva

23-11-2021

AECI

Juan A. Herrera Silva, Ph.D(c)
CDPSE, CISA, CRISC, CSXF, COBIT5, ISO27001LA

ESCUELA POLITÉCNICA NACIONAL

☑ ***Consultor Experto en Ciberseguridad – CEO en Level Technology***

Responsable líder de servicios de Auditoría Informática y Consultoría en Ciberseguridad, Seguridad de la Información, Ethical Hacking, Gestión de TI y Riesgos Tecnológicos.

- *Tiene 25 años de experiencia en Auditoría Informática y Seguridad de la Información, en importantes empresas nacionales y multinacionales de los sectores bancario, manufacturero, comercial, seguros, servicios y tecnología. Es CISO en una importante financiera y CISO Asesor de Ciberseguridad y Seguridad de la Información en varias empresas locales.*
- *Actualmente está culminando el* ***Doctorado en "Seguridad Informática"*** *en la EPN-FIS.*
- *Obtuvo en el 2020 el* ***Certified Data Privacy Solutions Engineer, CDPSE*** *(ISACA), Certificación Scrum Foundation Professional SFPC, Certificados AWS Security Fundamentals, AWS Cloud Audit, AWS Security – Identify and Compliance.*
- *Es MSc. en Ingeniería Eléctrica con mención en Conectividad y Redes de Telecomunicaciones. Posee un Diplomado Superior en Plataformas Operativas para Internetworking. Es Ingeniero de Sistemas graduado en la Escuela Politécnica Nacional.*
- *Ha liderado varios proyectos exitosos de SGSI con ISO 27001, BCP con ISO 22301, Auditorías especializadas de Seguridad Informática, Ethical Hacking y Evaluación de Riesgo Tecnológico en importantes instituciones financieras, seguros y comerciales.*
- *Posee Certificación como Auditor Líder en Sistemas de Gestión de Seguridad ISO 27001, Certificación COBIT 5 Foundation, Certificación en Ciberseguridad Fundamentos (CSXF).*
- *Obtuvo en el 2006 el Certified Information System Auditor, CISA y en el 2011 el Certified Risk Information System and Control, CRISC, dados por ISACA Internacional.*
- *Formación especializada en BIG DATA, Machine Learning, PMP y en Pruebas de Calidad de Software (ISTQB).*
- *Es especialista en gestión y seguridades de plataformas tecnológicas y Ethical Hacking.*
- ***Profesor Principal a Tiempo Parcial de la Facultad de Sistemas - Escuela Politécnica Nacional*** *de las Cátedras CISA y CISM desde 2010. Profesor invitado a cursos especializados de Auditoría Informática y Seguridad de la Información en varias universidades del país.*
- *Ex-Presidente y miembro fundador del Capítulo Quito, Ecuador - Information Systems Audit and Control Association (ISACA) y es Microsoft Certified Systems Administrator en ambientes de Redes Windows Server 2008, MCSA.*

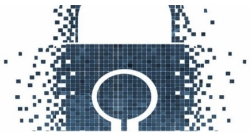
Perfil Profesional

Detección de Ransomware con Seguridad Cognitiva

Agenda:

1. Introducción
2. Familias y evolución
3. Estadísticas
4. Trabajo de Investigación Doctoral
   - Tipos de Análisis de Ransomware
   - Sandboxing
   - Hipótesis
   - Comportamiento.
   - Modelos para prevención
   - Hacia dónde vamos?

AECI



1. INTRODUCCIÓN AL RANSOMWARE

Concepto sobre ransomware

El ransomware se puede definir como un tipo de software malicioso o malware. El ransomware (secuestro de información) es el término genérico para referirse a todo tipo de software malicioso que le exige al usuario del equipo el pago de un rescate. Al concretar la infección puede bloquear el acceso al equipo o bien cifrar archivos para dejarlos inaccesibles.

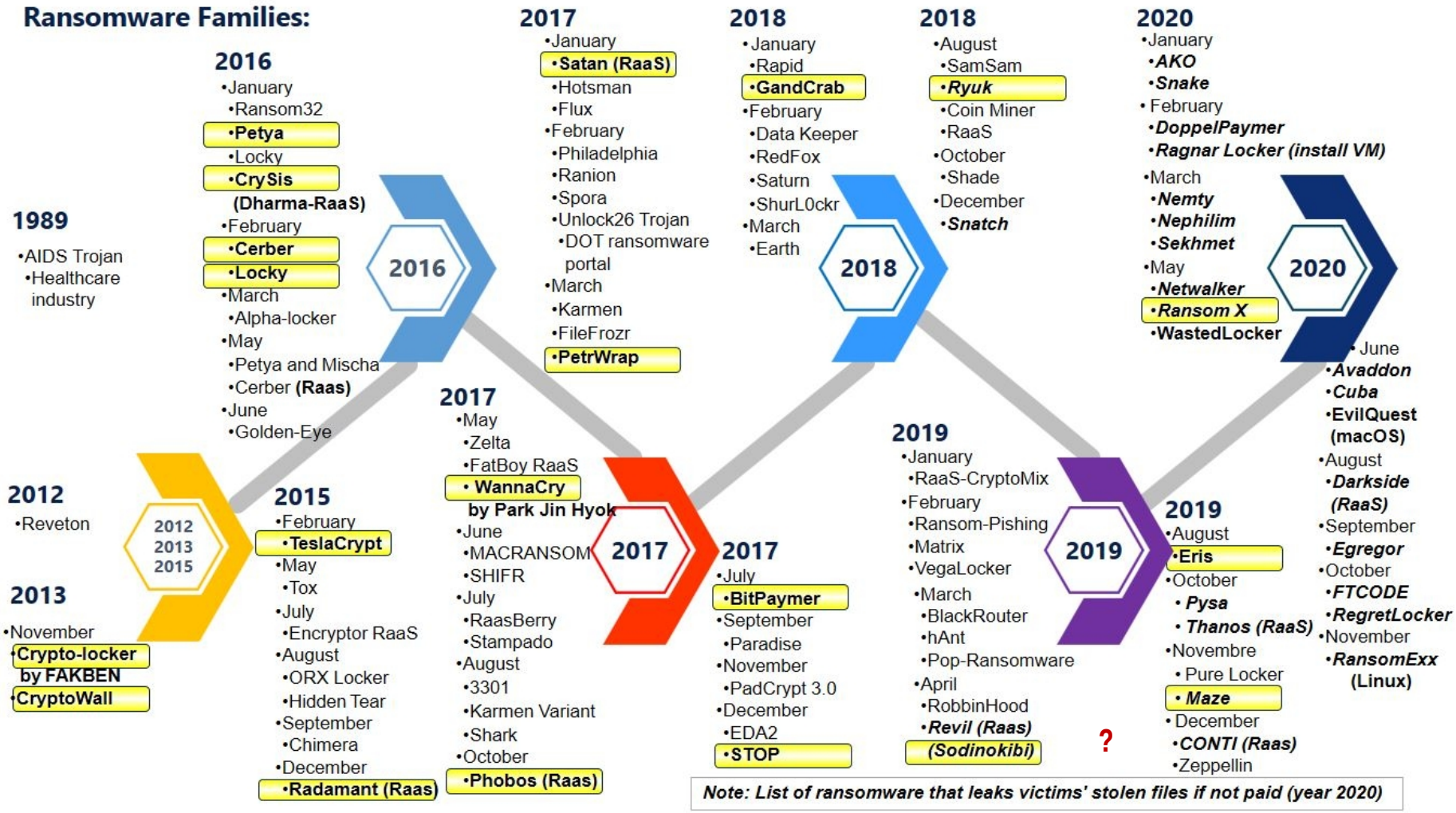
Historia del ransomware

Hace unos pocos años, todo cambió. Bitcoin se expandió y se hizo popular entre los ciberdelincuentes. La moneda cifrada es, simultáneamente, un activo digital y un sistema de pago imposible de rastrear o regular. Por supuesto, a los delincuentes les resultó útil, Además, se cambió a una nueva estrategia: en lugar de bloquear el acceso a los navegadores y a los sistemas operativos, comenzaron a cifrar los archivos de los discos duros de las víctimas.

En el año 2018 y 2019 existen ataques de Ransomware incluso a Sistemas Industriales (SCADA) para empresas de Agua Potable en USA.

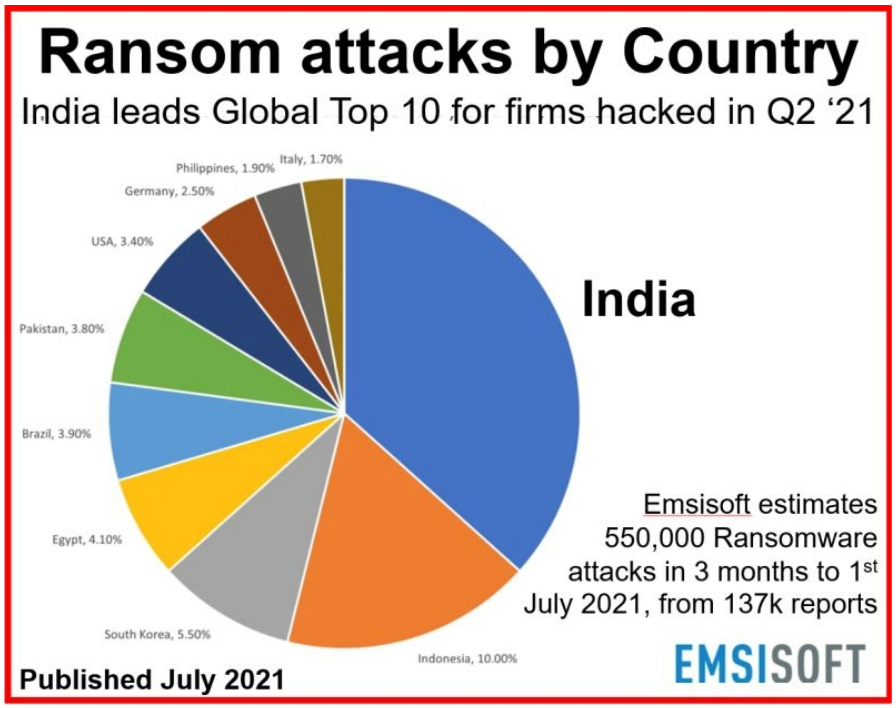
AECI

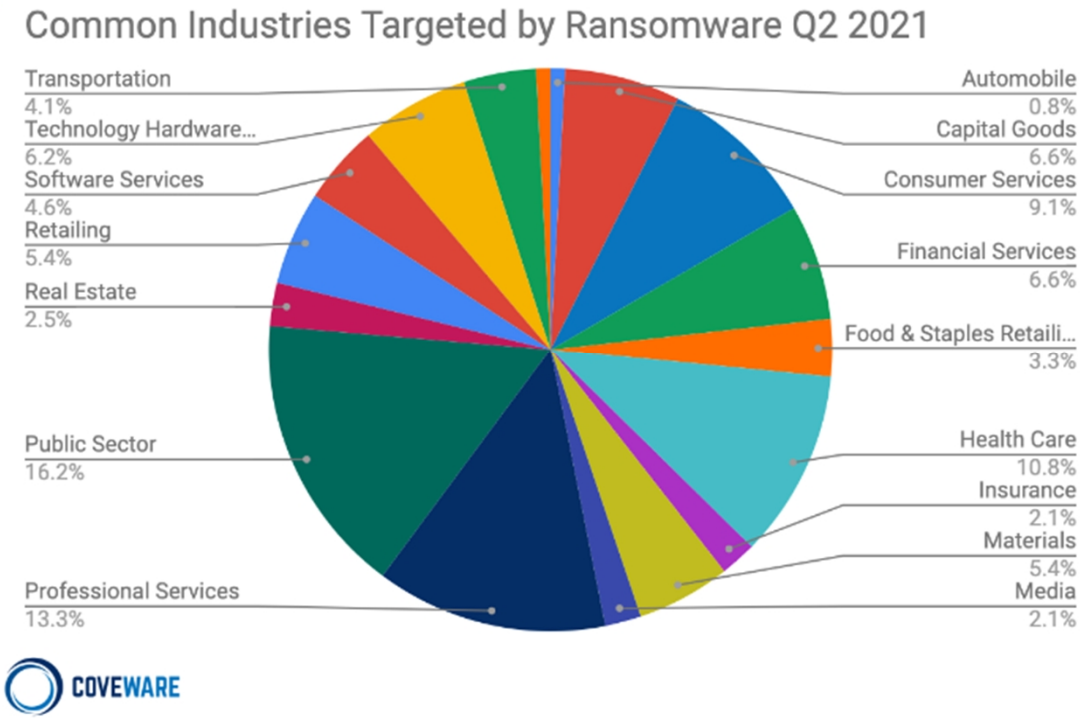
2. FAMILIAS Y EVOLUCIÓN DE RANSOMWARE



Elaborado por: Ph.D (c) Juan Herrera

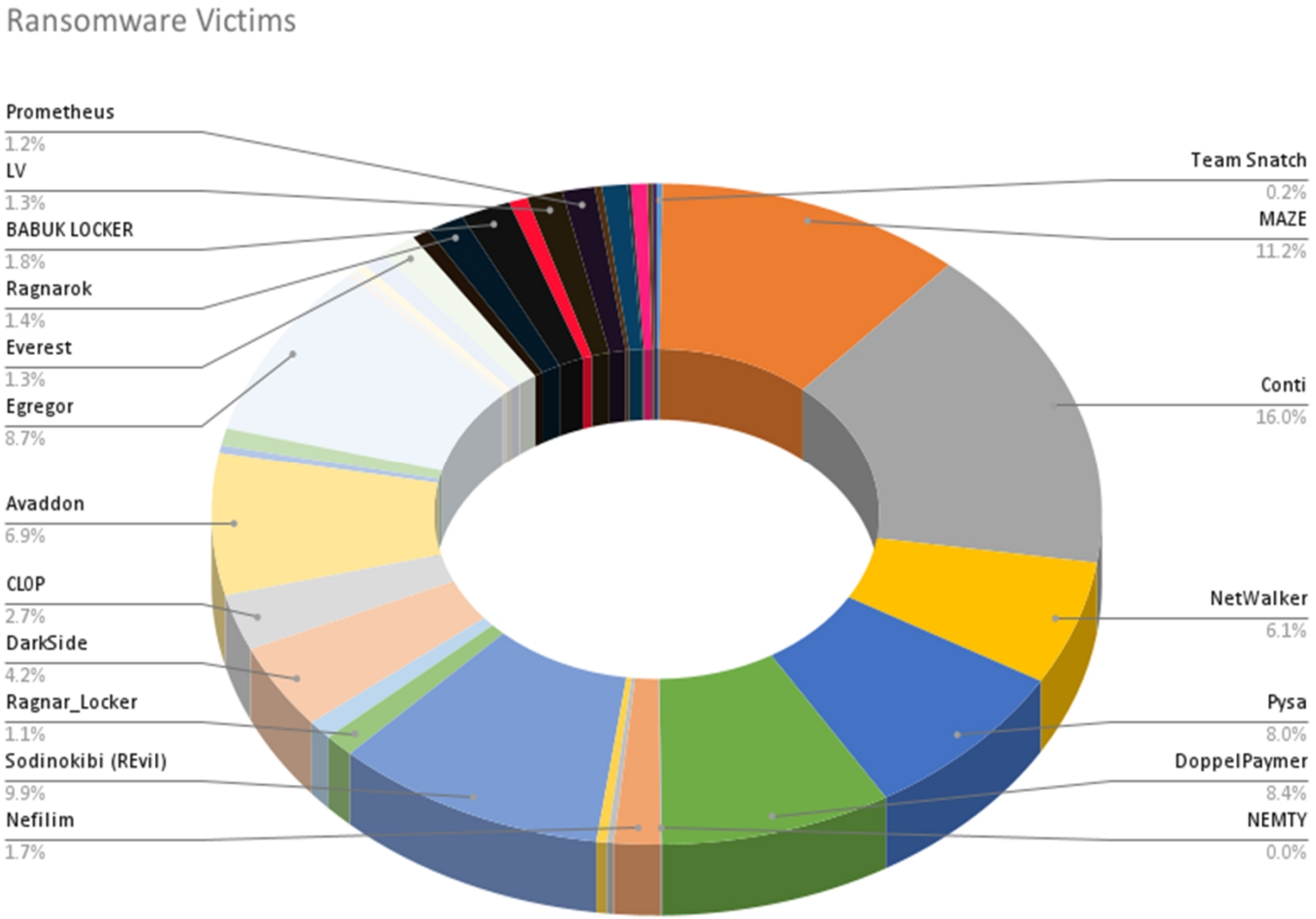
3. Ransomware: Estadísticas





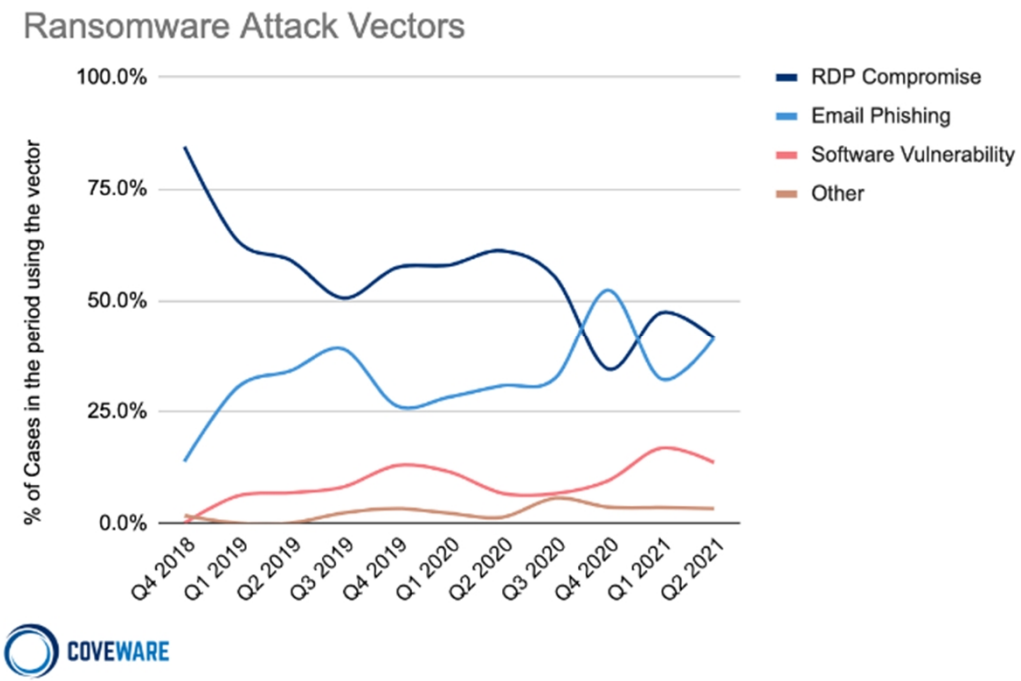
AECI

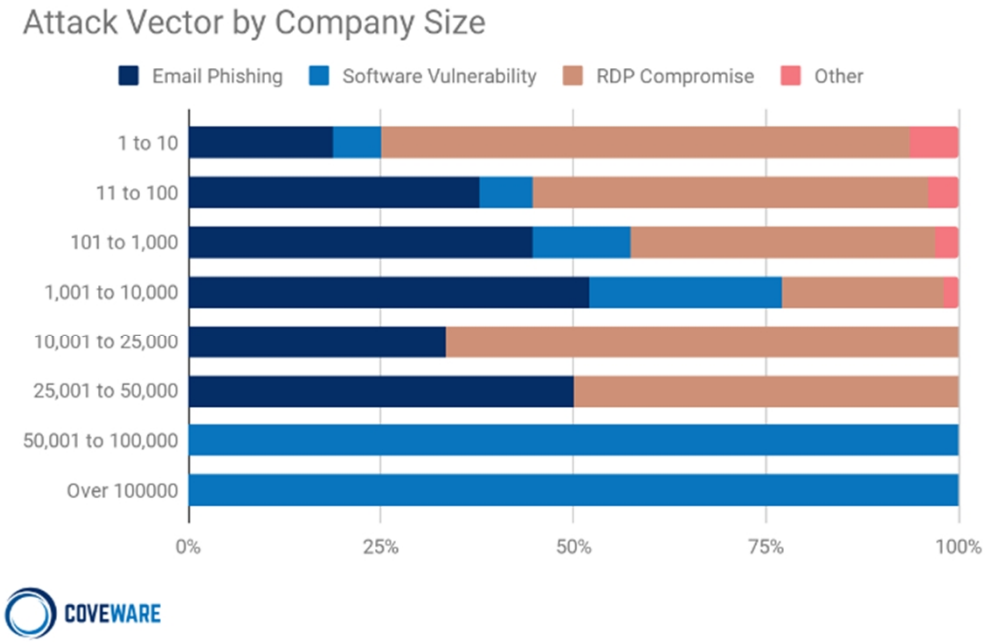
3. Ransomware: Estadísticas



AECI

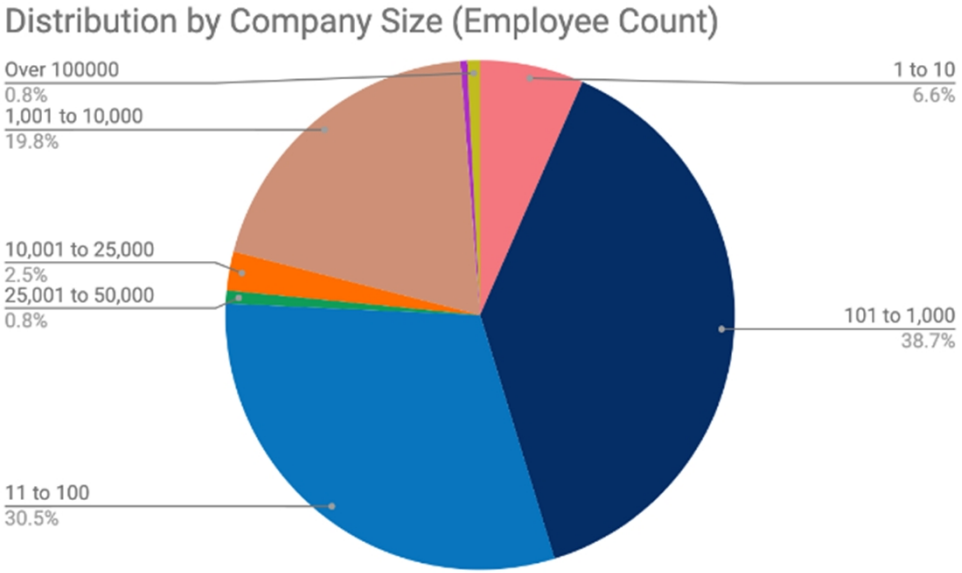
3. Ransomware: Estadísticas

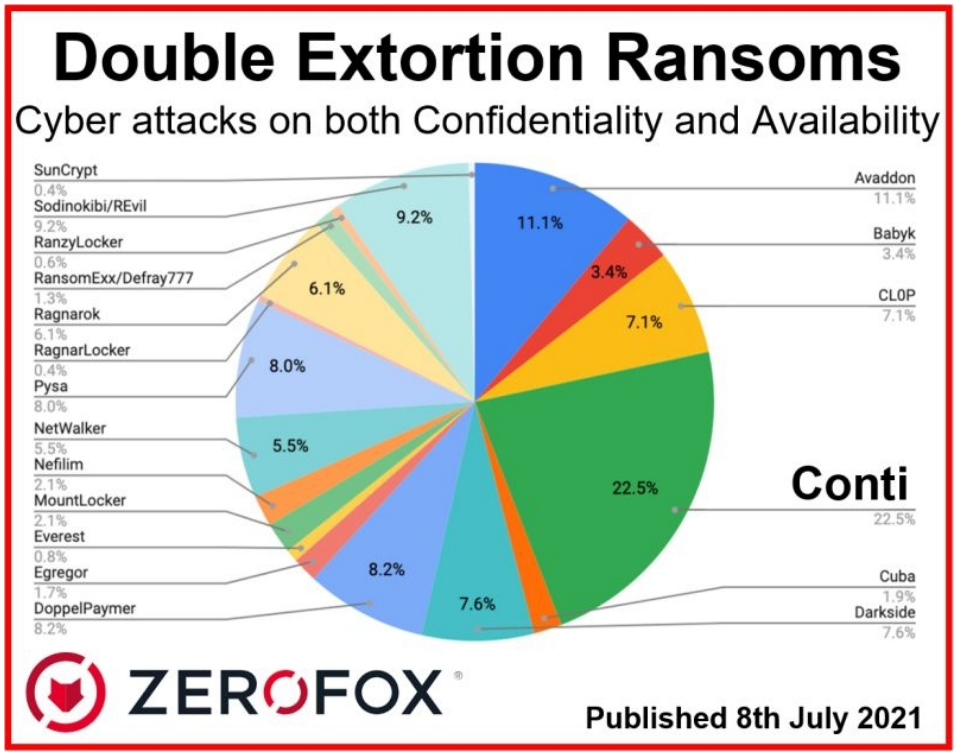




AECI

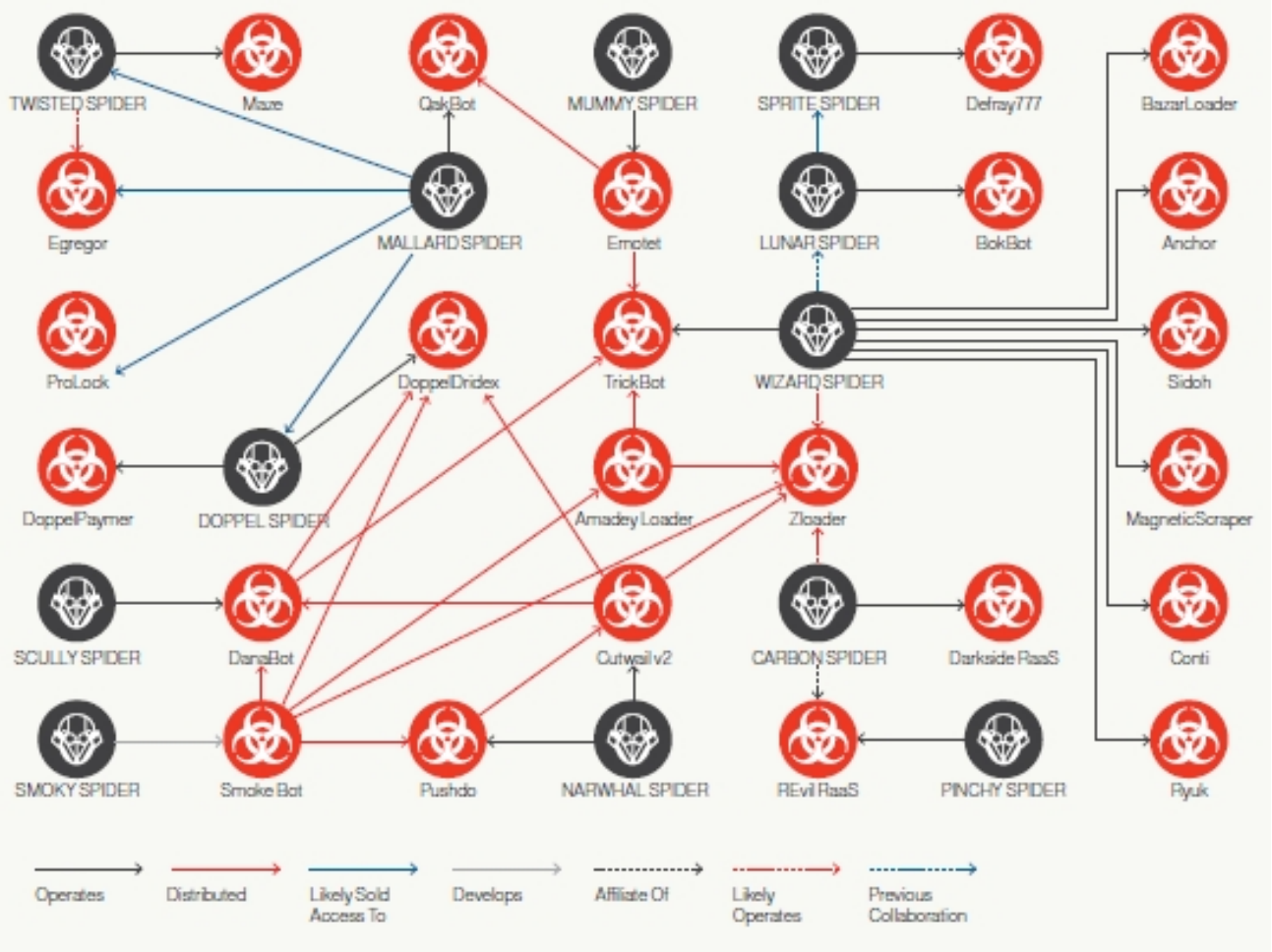
3. Ransomware: Estadísticas y Evolución



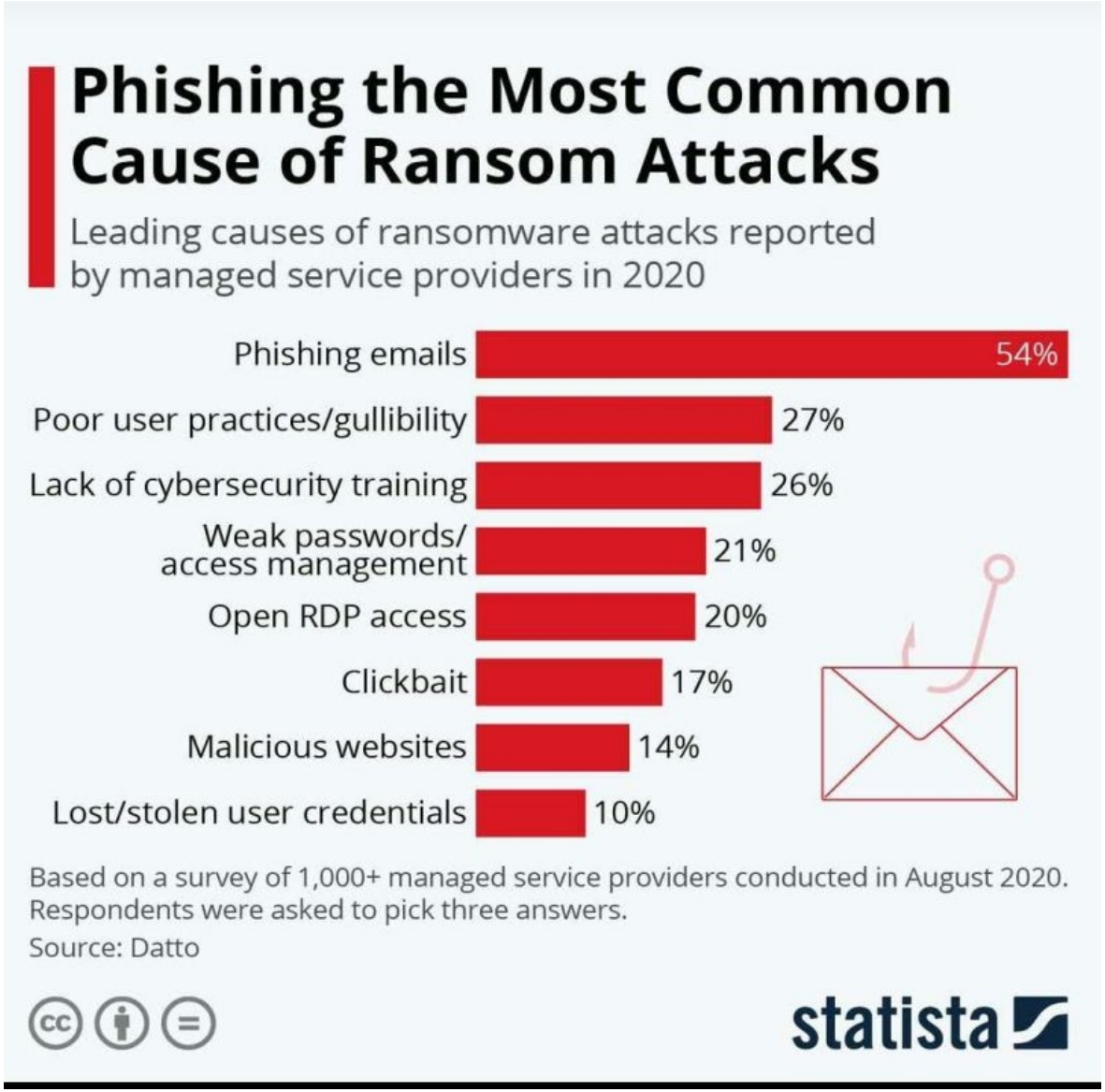


AECI

Observed eCrime Relationships in 2020

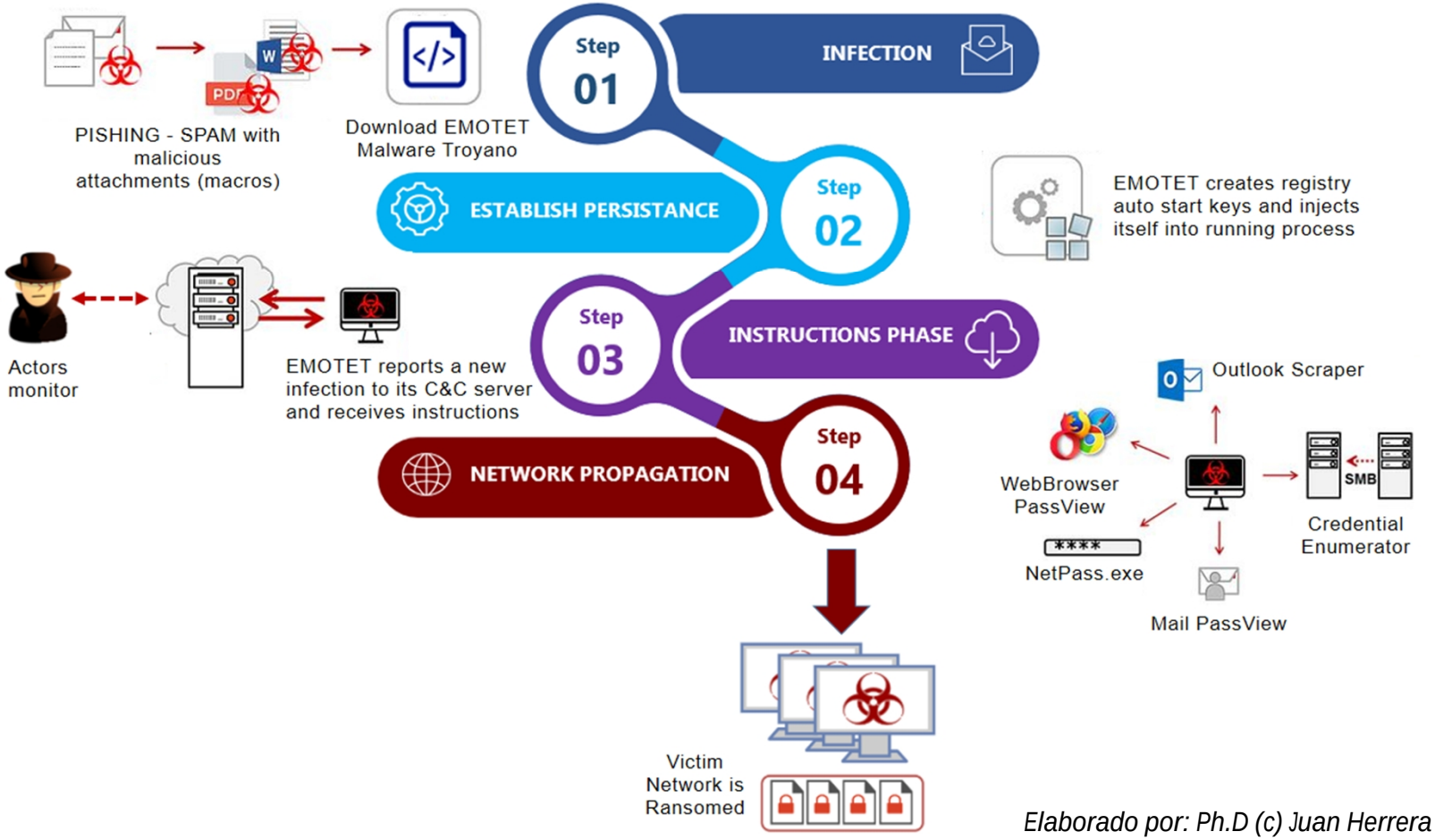


AECI


Phishing the Most Common Cause of Ransom Attacks
Leading causes of ransomware attacks reported by managed service providers in 2020
Phishing emails 54%
Poor user practices/gullibility 27%
Lack of cybersecurity training 26%
Weak passwords/ access management 21%
Open RDP access 20%
Clickbait 17%
Malicious websites 14%
Lost/stolen user credentials 10%
Based on a survey of 1,000+ managed service providers conducted in August 2020. Respondents were asked to pick three answers.
Source: Datto
statista

AECI

Ransomware by EMOTET Botnet Infection:



AECI

Elaborado por: Ph.D (c) Juan Herrera

TRABAJO DE INVESTIGACIÓN DOCTORAL

AECI

Técnicas y herramientas para el análisis de Ransomware

TIPOS DE ANÁLISIS DE RANSOMWARE

Análisis estático: En este análisis, el comportamiento del ransomware se examina estadísticamente mediante el estudio de su interacción con el entorno, los datos capturados, los archivos manipulados, las interrupciones de la red y puertos, y las actividades operativas, entre otras.

Análisis dinámico: Se lleva a cabo a través de un proceso de ingeniería inversa, donde el código malicioso del software se decodifica, examina, analiza y descompila. En este análisis, se emplean varias herramientas, como los depuradores, que analizan el código de software equivalente, y descompiladores, que convierten el ransomware en su código binario equivalente.

HERRAMIENTAS PARA EL ANÁLISIS

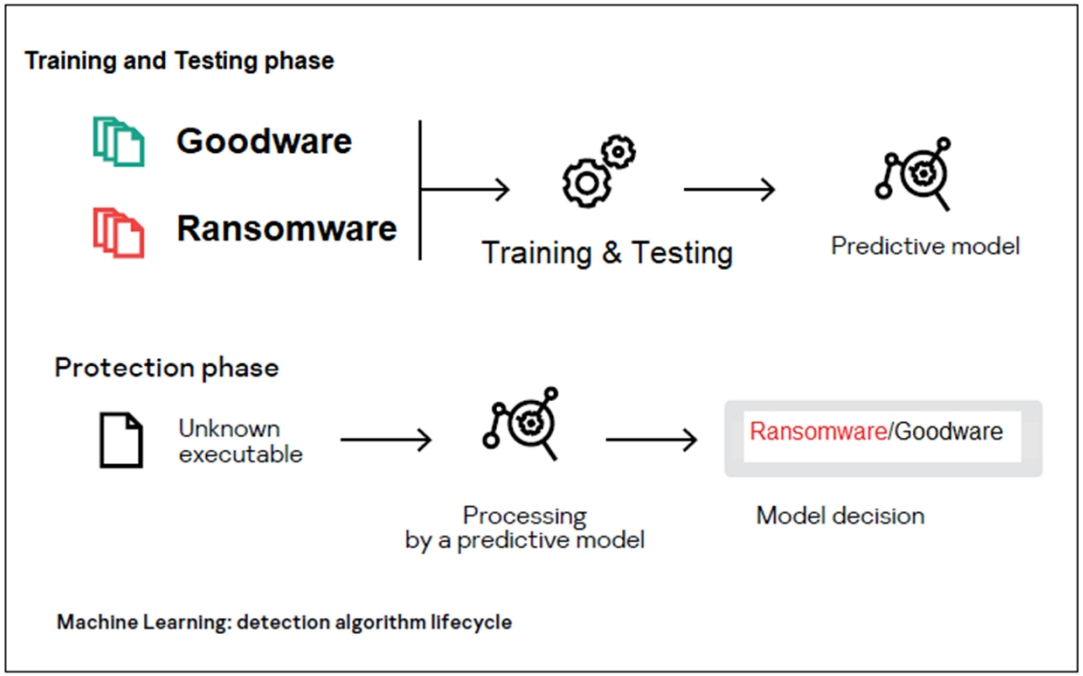
Sandboxing: Es la práctica de engañar a una aplicación o programa para que piense que se está ejecutando en una computadora normal y observar el comportamiento. A menudo se usa para ejecutar código no probado, o programas no confiables de terceros no verificados, proveedores, usuarios no confiables y sitios web que no son de confianza

Cuckoo Sandbox: **S**istema de análisis de malware. Significa que se puede lanzar cualquier archivo sospechoso en él y en cuestión de segundos Cuckoo va a entregar algunos resultados detallados que describen lo sucedido dentro de un entorno aislado

AECI

1. Research Hypothesis

Is it possible to build a dataset containing goodware and typical ransomware samples that allow building machine learning models that achieve early detection of this threat to minimize the damage it can cause?



AECI

2. MITRE ATT&CK Matrix for Ransomware

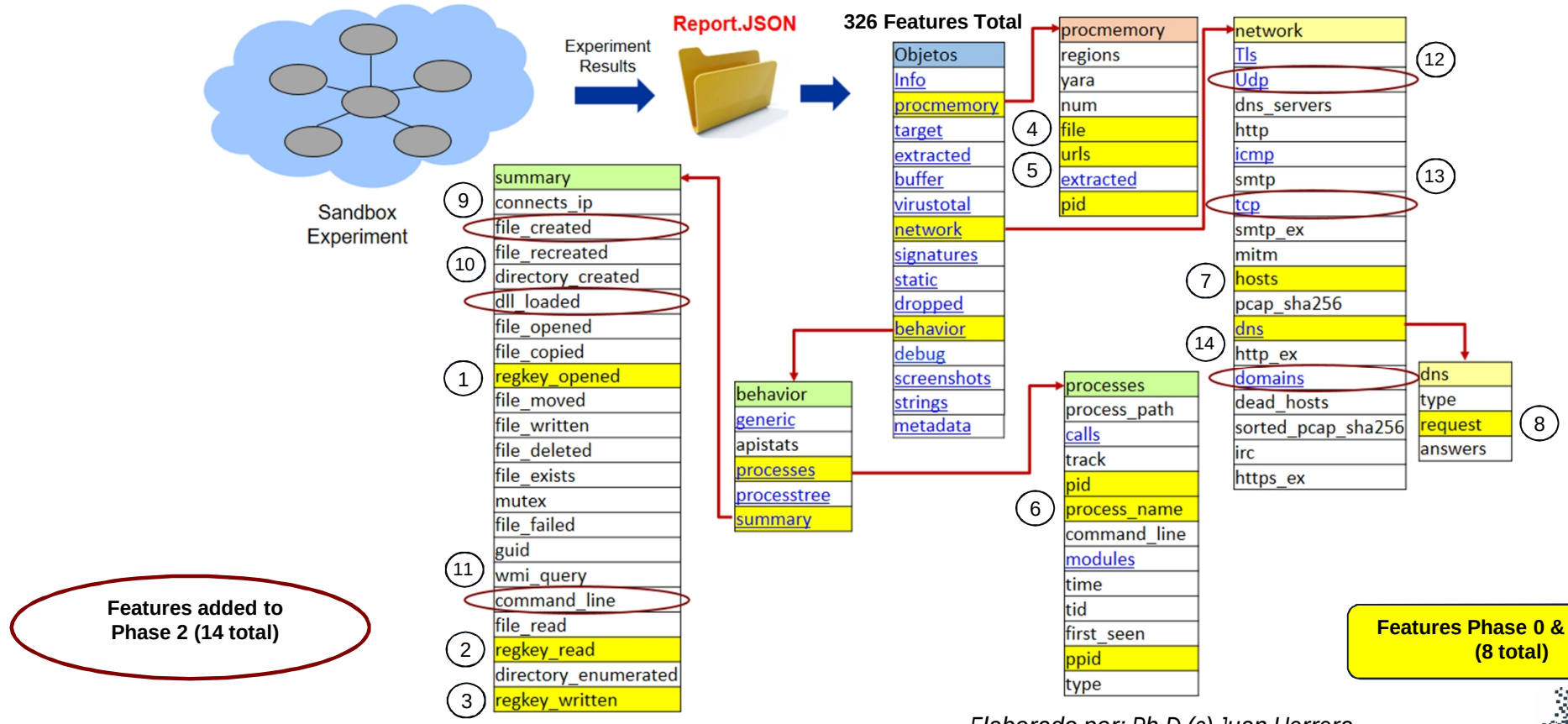
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise (T1189)	User Execution (T1204)	Registry Run Keys / Startup Folder (T1060)	Valid Accounts (T1078)	Disabling Security Tools (T1089)	Brute Force (T1110)	Network Service Scanning (T1046)	Remote Desktop Protocol (T1076)	Data from Local System (T1005)	Remote Access Tools (T1219)	Transfer Data to Cloud Account (T1537)	Data Encrypted for Impact (T1486)
External Remote Services (T1133)	PowerShell (T1086)	External Remote Services (T1133)	Exploitation for Privilege Escalation (T1068)	Group Policy Modification (T1484)	Credential Dumping (T1003)	Network Share Discovery (T1135)	Windows Admin Shares (T1077)	Data from Network Shared Drive (T1039)	Remote File Copy (T1105)	Exfiltration Over Other Network Medium (T1011)	Inhibit System Recovery (T1490)
Spearphishing Attachment (T1193)	Command-Line Interface (T1059)	Create Account (T1136)		Redundant Access (T1108)	Credentials in files (T1081)	Remote System Discovery (T1018)	Windows Remote Management (T1028)		Multi-hop Proxy (T1188)	Data Encrypted (T1022)	Resource Hijacking (T1496)
Spearphishing Link (T1192)	Scripting (T1064)	Scheduled Task (T1053)		Masquerading (T1036)	Credentials from Web Browsers (T1503)	System Information Discovery (T1082)				Exfiltration Over Command and Control Channel (T1041)	
Valid Accounts (T1078)	Windows Management Instrumentation (T1047)	Valid Accounts (T1078)		Bypass User Account Control (T1088)		Permission Groups Discovery (T1069)					
Supply Chain Compromise (T1195)	Exploitation for Client Execution(T1203)	New Service (T1050)		NTFS File Attributes (T1096)		Password Policy Discovery (T1201)					
Trusted Relationship (T1199)	Mshta (Mshta)	Modify Existing Service (T1031)		Obfuscated Files or Information (T1027)		Domain Trust Discovery (T1482)					
Exploit Public-Facing Application (T1190)	Scheduled Task (T1053)	WMI Event Subscription (T1084)		Deobfuscate/ Decode Files or Information (T1140)		Network Configuration (T1016)					
				File and Directory Permissions Modification (T1222)							
				File Deletion (T1107)							

Ref: Ransomware 2020 Analysis, Group-IB

ATT related to Dataset features of Phase 2

AECI

3. Test setting - Features analyzed for the Dataset



Elaborado por: Ph.D (c) Juan Herrera

AECI

3.1 Procmemory, Network and Behavior objects

Object	Description	Feature	Explanation	Observation
PROCMEMORY	It allows the creation of memory dumps for each analyzed process (before they finish or before the analysis ends).	File	File created as a memory dump	Feature chosen because the file runs in memory. Phase 0 and 1.
		Urls	Urls generated during the execution of memory processes	Feature chosen because it stores in memory a list of urls that can be filtered to blacklists. Phase 0 and 1.
		pid	Process identifier	Feature chosen because it identifies the generated file (File). Phase 0 and 1.
NETWORK	Includes information on the network infrastructure used during the analyses.	hosts	hosts involved in the analysis. Help create blacklists	Feature chosen because of the communication that exists with a malicious host. You can create blacklists. Phase 0 and 1.
		dns	DNS servers involved in the analysis	Feature chosen due to communication with external domain servers. DNS sub-characteristics (request). Phase 0 and 1.
		domain	Domains involved in communication	Feature chosen due to communication with other domains. DOMAIN sub-characteristics. Phase 2.
		tcp	network analysis of the tcp protocol	Feature chosen due to the use of communication via tcp protocol. TCP sub-characteristics. Phase 2.
		udp	network analysis of the udp protocol	Characteristic chosen due to the use of communication via udp protocol. Sub characteristics UDP. Phase 2.

Report.JSON

Object	Description	Feature	Explanation	Observation
BEHAVIOR	It allows to see the behavior of ransomware, that is, to see the processes that the ransomware performs, libraries to which it makes calls, registry keys that affect	Processes	Processes carried out by the device	Feature chosen because processes modify the infected system. Selected sub-characteristics Processes (ppid, pid and process_name). Phase 0 and 1.
		Summary	Summary of files, log keys, directories and commands involved during the execution of processes	Feature chosen because it contains parameters that affect infected systems. The sub-charactistics summary (regKeys) has been chosen. Phase 0, 1 and 2. Also, the sub-characteristics (file_created, dll_loaded, and command_line) have been chosen. Phase 2

AECI

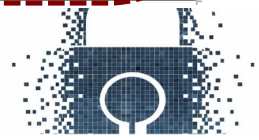
3.2 Test setting – Obtained a balanced Dataset

OBJECT	FEATURE	CRITERION
Behavior	regkey_opened	Feature taken because of the changes they make in the OS Part of Phase 1.
Behavior	regkey_read (1)	Feature taken because of the changes they make in the OS Part of Phase 1& 2
Behavior	regkey_written	Feature taken because of the changes they make in the OS Part of Phase 1.
Behavior	processes	Feature taken because of the processes running on the OS Part of Phase 1.
Procmemory	files	Feature taken because of files created by memory processes. Part of Phase 1.
Procmemory	urls	Feature taken due to urls created by memory processes. Part of Phase 1.

OBJECT	FEATURE	CRITERION
Network	hosts	Feature taken due to communication of hosts involved. Part of Phase 1.
Network	request	A feature took due to communication to domain servers (requests). Part of Phase 1.
Behavior	file_created (1)	A feature took because of the files that are created by the artifact in the OS Part of Phase 2
Behavior	dll_loaded (2)	Characteristic took because of the dlls that load the artifact during its execution. Part of Phase 2.
Behavior	command_line (3)	A feature taken because of the commands the artifact uses. Part of Phase 2.
Network	domains (4)	A feature took because of domains involved in communication. Part of Phase 2.
Network	tcp (5)	A feature taken due to network analysis of the tcp protocol. Part of Phase 2.
Network	udp (1)	A feature taken due to network analysis of udp protocol. Part of Phase 2.

(n) Selected features to Predictive Models

AECI



3.3 Test setting - Artifacts for Dataset

ID	NAME	SHA1	MD5	TIPO	FAMILY	EXPERIMENTS
1	7-ZipPortable_9.20_Rev_2.paf.exe	35bcca0e8b907386ca4c7536dc55913e3c71b220	7fa4441c55a838e0691328cebde21802	PE32 executable (GUI) Intel 80386, for MS Windo	G	20
2	AdbeRdr11008_es_ES.exe	aa08e431163c6129697d0aae7f4f9915bc90b2ba	3472d1522f9568534a9116400af1a1be	PE32 executable (GUI) Intel 80386, for MS Windo	G	10
3	AcroRdrDC1901220036_es_ES.exe	ad998431b1ec06b2ea2087e3a2ebc65a6d23ba9e	153311a588cbbc6f45ea4401bf081fec	PE32 executable (GUI) Intel 80386, for MS Windo	G	10
4	cerber.exe	c69a0f6c6f809c01db92ca658fcf1b643391a2b7	8b6bc16fd137c09a08b02bbe1bb7d670	PE32 executable (GUI) Intel 80386, for MS Windo	E	20
5	chrome.exe	04ca28f529aae1db4be4cfb4c601f57c7d08f997	da2965d0020f4156141c783ebcd64f0f	PE32 executable (GUI) Intel 80386, for MS Windo	G	20
6	cryptolocker.exe	65559245709fe98052eb284577f1fd61c01ad20d	04fb36199787f2e3e2135611a38321eb	PE32 executable (GUI) Intel 80386, for MS Windo	E	20
7	cryptowall.bin	ca963033b9a285b8cd0044df38146a932c838071	47363b94cee907e2b8926c1be61150c7	PE32 executable (GUI) Intel 80386, for MS Windo	E	20
8	dllhost.exe	ab0af67fd000646ed231ee421e5c71798d0d86a0	0f886de058726bb6323bfd98773fad26	PE32 executable (GUI) Intel 80386, for MS Windo	G	10
9	dllhost.exe	ace762c51db1908c858c898d7e0f9b36f788d2d9	a63dc5c2ea944e6657203e0c8edeaf61	PE32 executable (GUI) Intel 80386, for MS Windo	G	10
10	explorer.exe	78f905f135771dec9646f6f753195adf5e7bf7c9	7522f548a84abad8fa516de5ab3931ef	PE32 executable (GUI) Intel 80386, for MS Windo	G	10
11	explorer.exe	84123a3decdaa217e3588a1de59fe6cee1998004	38ae1b3c38faef56fe4907922f0385ba	PE32+ executable (GUI) x86-64, for MS Windows	G	10
12	firefox.exe	efe760ee6f516adb01e3092e78bda904df908b56	9adcb5abe8bb7e1a9355632817d23f43	PE32 executable (GUI) Intel 80386, for MS Windo	G	20
13	locky	b606aaa402bfe4a15ef80165e964d384f25564e4	b06d9dd17c69ed2ae75d9e40b2631b42	PE32 executable (GUI) Intel 80386, for MS Windo	E	20
14	Petrwrap.exe	34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d	71b6a493388e7d0b40c83ce903bc6b04	PE32 executable (DLL) (console) Intel 80386, for	L	20
15	petya.bin	d1c62ac62e68875085b62fa651fb17d4d7313887	a92f13f3a1b3b39833d3cc336301b713	PE32 executable (GUI) Intel 80386, for MS Windo	L	20
16	radamant.ViR	05ae9c76f8f85ad2247c06d26a88bbbcfff4d62e	6152709e741c4d5a5d793d35817b4c3d	PE32 executable (GUI) Intel 80386 (stripped to ex	E	20
17	satana.bin	5b063298bbd1670b4d39e1baef67f854b8dcba9d	46bfd4f1d581d7c0121d2b19a005d3df	PE32 executable (GUI) Intel 80386, for MS Windo	L	20
18	services.exe	7cf0d257861a23191a9d482a51783593d6a64f74	d658a8c2fc7b2ad53d1259741a09ee04	PE32 executable (GUI) Intel 80386, for MS Windo	G	10
19	services.exe	ff658a36899e43fec3966d608b4aa4472de7a378	71c85477df9347fe8e7bc55768473fca	PE32+ executable (GUI) x86-64, for MS Windows	G	10
20	svchost.exe	1aae36311da414c8fd5b32956aaed1d82237ab08	4f2340f0bd5b6365c38e74dd391919a8	PE32 executable (GUI) Intel 80386, for MS Windo	G	10
21	svchost.exe	4af001b3c3816b860660cf2de2c0fd3c1dfb4878	54a47f6b5e09a77e61649109c6a08866	PE32 executable (GUI) Intel 80386, for MS Windo	G	10
22	teslacrypt	51b4ef5dc9d26b7a26e214cee90598631e2eaa67	6e080aa085293bb9fbdcc9015337d309	PE32 executable (GUI) Intel 80386 (stripped to ex	E	20
23	wannacry.exe	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467	84c82835a5d21bbcf75a61706d8ab549	PE32 executable (GUI) Intel 80386, for MS Windo	E	20
24	WinRAR.EXE	0d95c17831e9cd4d0d7efb9efa866437eed186fd	b78d7b5d2fcbe1171a3500cc2176f9c9	PE32 executable (GUI) Intel 80386, for MS Windo	G	20
					TOTAL	380

Artifacts Directory:
https://github.com/ytisf/theZoo/tree/master/malwares/Binaries
https://www.exefiles.com/en/

FAMILY:

G: Goodware / E: Encriptor / L: Locker

AECI

4. Results (Dataset & Features Selection)

Best Features

Phase 2

ID	FEATURES
5F1	(regkey_read, udp, file_created), dll_loaded, comand_line, domain, tcp
4F1	(regkey_read, udp, file_created), command_line, domain, tcp
4F2	(regkey_read, udp, file_created), dll_loaded, command_line, domain
4F3	(regkey_read, udp, file_created), dll_loaded, command_line, tcp
4F4	(regkey_read, udp, file_created), dll_loaded, domain, tcp
4F5	dll_loaded, comand_line, domain, tcp
3F1	(regkey_read, udp, file_created), comand_line, domain
3F2	(regkey_read, udp, file_created), comand_line, tcp
3F3	(regkey_read, udp, file_created), dll_loaded, comand_line
3F4	(regkey_read, udp, file_created), dll_loaded, domain
3F5	(regkey_read, udp, file_created), dll_loaded, tcp
3F6	(regkey_read, udp, file_created), domain, tcp
3F7	comand_line, domain, tcp
3F8	dll_loaded, comand_line, domain
3F9	dll_loaded, comand_line, tcp
3F10	dll_loaded, domain, tcp
2F1	(regkey_read, udp, file_created), comand_line
2F2	(regkey_read, udp, file_created), dll_loaded
2F3	(regkey_read, udp, file_created), domain
2F4	(regkey_read, udp, file_created), tcp
2F5	comand_line, domain
2F6	comand_line, tcp
2F7	dll_loaded, comand_line
2F8	dll_loaded, domain
2F9	dll_loaded, tcp
2F10	domain, tcp
1F1	(regkey_read, udp, file_created)
1F2	comand_line
1F3	dll_loaded
1F4	domain
1F5	tcp

See MITRE ATT&CK Matrix - Dataset features of Phase 2

AECI

4. Results (Dataset) – Performance Models

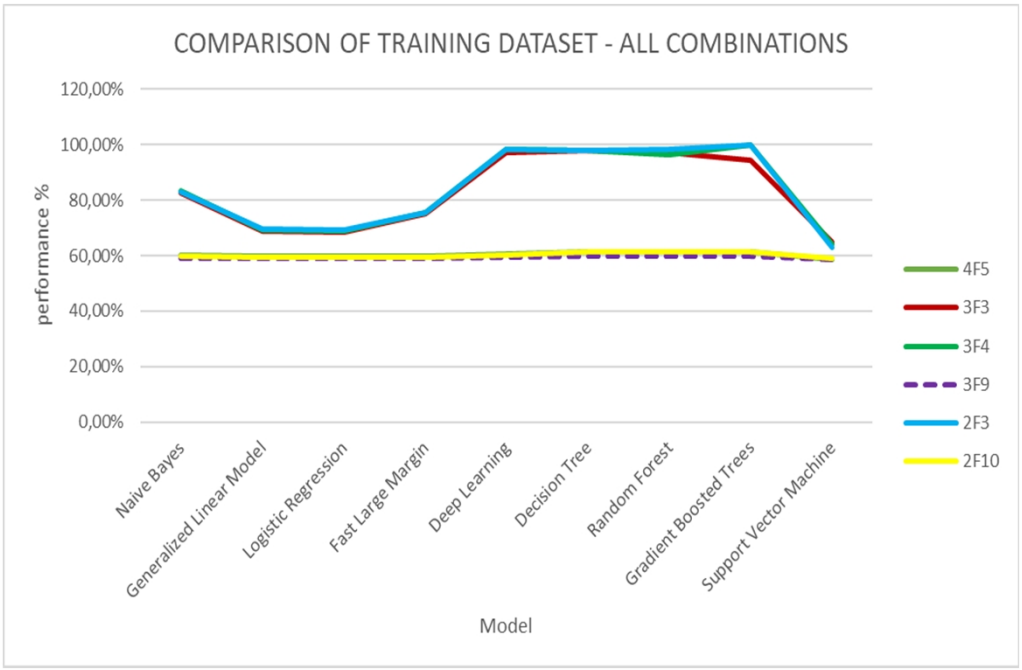
CHARACTERISTICS	ALGORITHM / MODEL	Accuracy training	Presicion training	Recall training	Classification Error training	Accuracy testing	Presicion testing	Recall testing	Classification Error testing
(regkey_read, udp, file_created), comand_line, domain	Gradient Boosted Trees	99,72%	99,82%	98,48%	0,28%	99,67%	99,81%	98,11%	0,33%
(regkey_read, udp, file_created), comand_line, tcp	Gradient Boosted Trees	98,48%	99,12%	97,37%	1,52%	98,38%	99,10%	96,94%	1,62%
(regkey_read, udp, file_created), dll_loaded, comand_line	Gradient Boosted Trees	94,48%	99,12%	97,38%	1,52%	98,38%	99,10%	96,94%	1,62%
(regkey_read, udp, file_created), dll_loaded, domain	Gradient Boosted Trees	99,73%	99,82%	98,48%	0,27%	99,67%	99,81%	98,11%	0,33%
(regkey_read, udp, file_created), dll_loaded, tcp	Gradient Boosted Trees	98,48%	99,13%	97,38%	1,52%	98,38%	99,10%	96,94%	1,62%
(regkey_read, udp, file_created), domain, tcp	Gradient Boosted Trees	99,72%	99,80%	98,48%	0,28%	99,68%	99,81%	98,11%	0,32%
comand_line, domain, tcp	Random Forest	61,35%	86,24%	36,54%	38,65%	61,14%	86,63%	36,72%	38,86%
dll_loaded, comand_line, domain	Random Forest	61,39%	86,69%	36,23%	38,61%	61,17%	83,23%	36,39%	38,83%
dll_loaded, comand_line, tcp	Random Forest	59,85%	86,10%	35,21%	40,15%	59,64%	86,42%	35,23%	40,36%
dll_loaded, domain, tcp	Random Forest	61,52%	86,81%	36,73%	38,48%	61,30%	86,67%	36,86%	38,70%

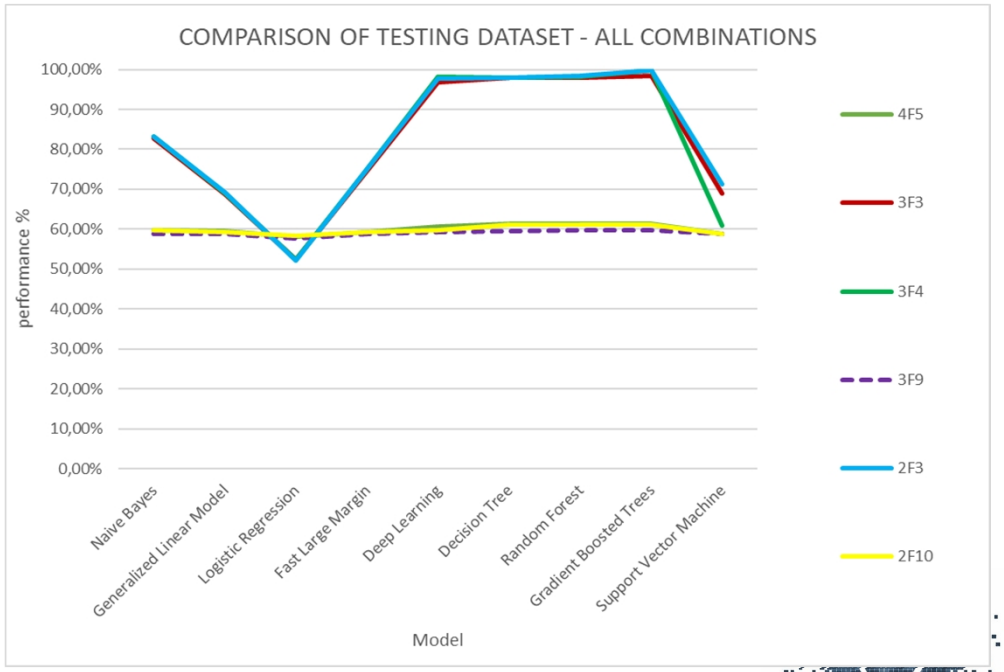
Best Results → Phase 2

$$True\ positive\ rate\ (TPR) = \frac{TP}{TP+FN}$$
$$False\ positive\ rate\ (FPR) = \frac{FP}{FP+TN}$$
$$Precision = \frac{TP}{TP+FP}$$
$$Recall = \frac{TP}{TP+FN}$$
$$F\text{-}measure = \frac{2 * Precision * Recall}{Precision + Recall}$$
$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}$$

AECI

4. Results (Dataset & Models)





AECI

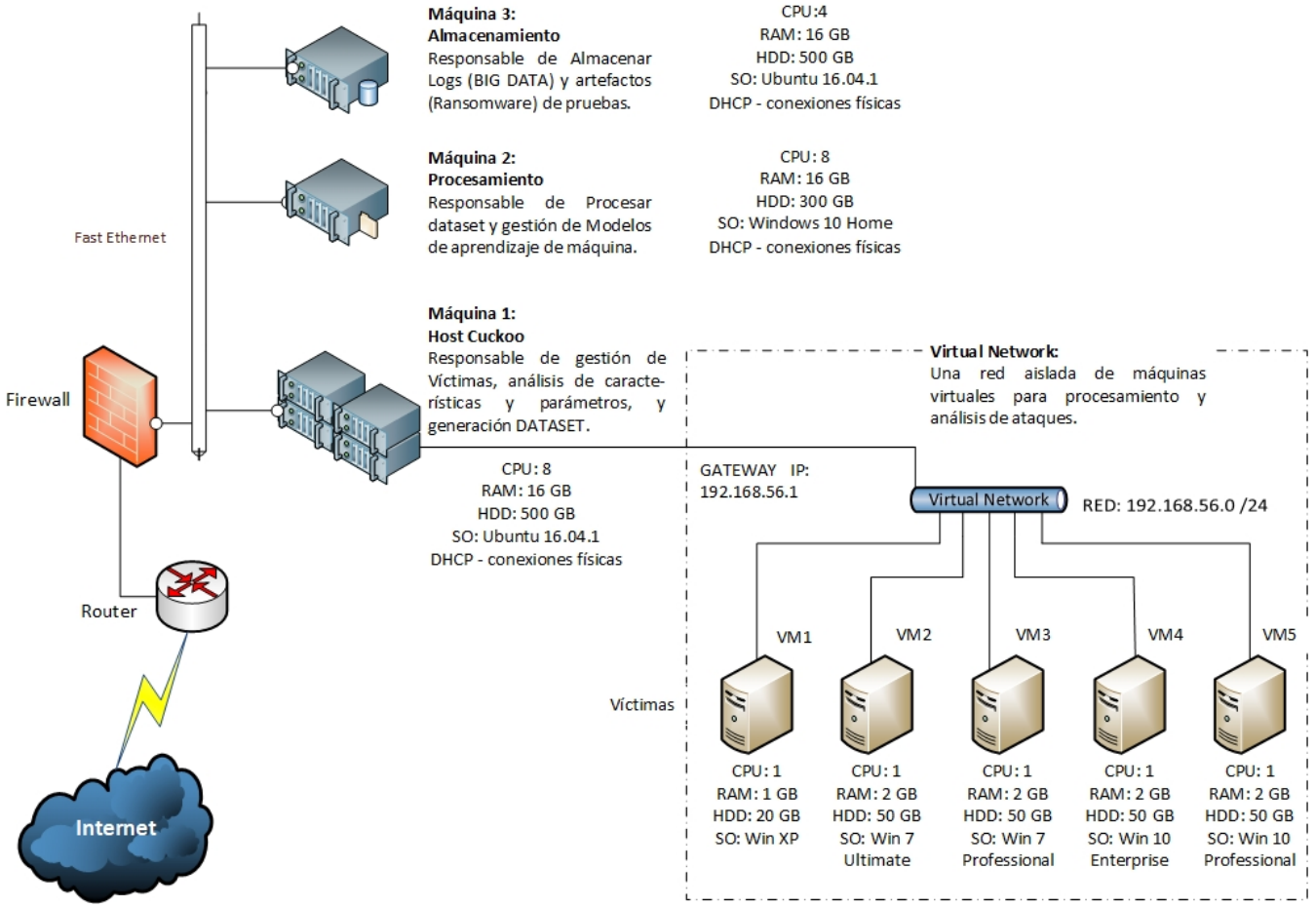
Trabajo de Investigación Doctoral

¿HACIA DÓNDE VAMOS?

(Mejores Modelos de Prevención)

AECI

Nuevo ambiente de Experimentación para Dataset



Elaborado por: Ph.D (c) Juan Herrera

Nuevos artefactos para Experimentación Dataset

ID	ARTEFACTO	FAMILIA	TIEMPO DE EXPERIMENTACIÓN USADO POR ARTEFACTO	OBSERVACIONES
1	7Zip	Goodware	8863	Artefacto Goodware seleccionado debido a su comportamiento de encripción y cifrado de archivos
2	Administrador de tareas (Taskmgr)	Goodware	15092	Artefacto Goodware seleccionado debido al acceso que tiene a procesos y tareas de sistema
3	API WINDOWS SECURITY CRYPTOGRAPHY (cipher)	Goodware	18455	Artefacto Goodware seleccionado debido a que realiza cifrado de archivos del sistema operativo
4	API WINDOWS SYSTEM INFORMATION REGISTRY (regedit)	Goodware	18075	Artefacto Goodware seleccionado debido a que interactúa con las claves de registro
5	API WINDOWS VOLUME MANAGEMENT (diskpart)	Goodware	20973	Artefacto Goodware seleccionado debido a su acceso a volumenes y particiones
6	Bitlocker	Goodware	8625	Artefacto Goodware selecionado debido a que cifra discos y/o carpetas que se deseen
7	BitPaymer	Encryptor	8852	
8	Cerber	Encryptor	45937	
9	cmd	Goodware	42852	Artefacto Goodware seleccionado debido a que dentro de este se pueden ejecutar scripts o comandos
10	Cryptolocker	Encryptor	50959	
11	Cryptowall	Encryptor	51367	
12	Crysis	Encryptor	69458	
13	dllhost	Goodware	43604	Artefacto Goodware seleccionado debido a su acceso al manejo de dlls durante diferentes etapas de uso de software. (ejecución, instalación, etc)
14	Eris	Encryptor	57963	
15	Escritorio Remoto de Windows	Goodware	21389	Artefacto Goodware seleccionado debido a la interacción de control que se puede tener con permisos otorgados sobre este
16	GandCrab	Encryptor	51564	
17	gpg	Goodware	54911	Artefacto Goodware seleccionado debido a que se realiza cifrados de llaves púlicas y privadas
18	IPScan	Goodware	56128	Artefacto seleccionado debido a a que permite realizar escaneo de direcciones IP en distintos ambientes
19	Locky	Encryptor	50926	
20	Maze	Encryptor	56764	

AECI

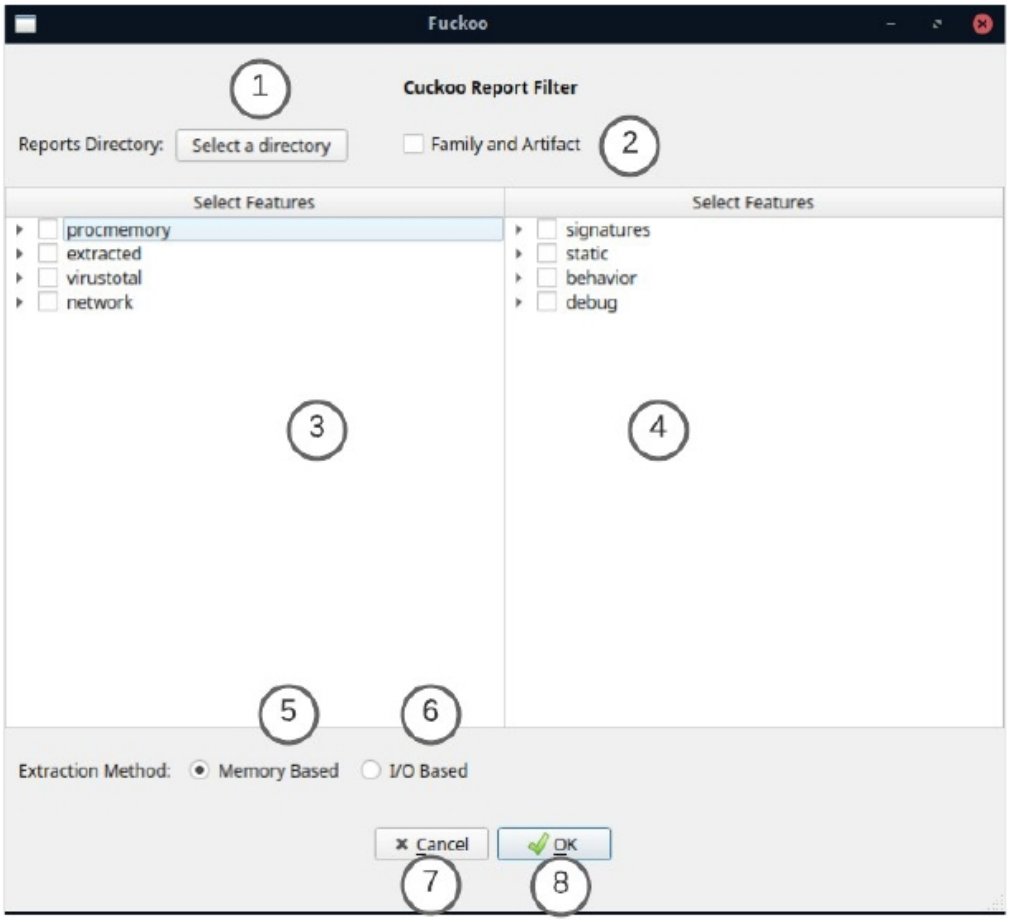
Nuevos artefactos para Experimentación Dataset

ID	ARTEFACTO	FAMILIA	TIEMPO DE EXPERIMENTACIÓN USADO POR ARTEFACTO	OBSERVACIONES
21	Microsoft SQL Server Compact	Goodware	52251	Artefacto seleccionado debido a que a su uso para getión de bases de datos
22	Nmap	Goodware	45927	Artefacto Goodware seleccionado debido a que permite realizar escaneos de disticntos parametros tales como puertos abiertos, direcciones ip entre otros
23	Petrwrap	Locker	47404	
24	Petya	Locker	49640	
25	Phobos	Encryptor	75790	
26	Radamant	Encryptor	55138	
27	RansomX	Encryptor	58813	
28	Ryuk	Locker	64178	
29	Satana	Locker	56424	
30	services	Goodware	53248	Artefacto Goodware seleccionado debido a sus interacción con servicios del sistema operativo
31	Sodinokibi	Encryptor	57347	
32	STOP	Encryptor	55898	
33	svchost	Goodware	49379	Artefacto Goodware seleccionado debido a que comprueba el sistema opeartivo y en la mayor parte de ocaciones es la principal víctima de ataques de malware
34	Team Viewer	Goodware	55569	Artefacto Goodware seleccionado debido a su interacción de control remoto
35	Teslacrypt	Encryptor	59166	
36	VNC	Goodware	47870	Artefacto Goodware seleccionado debido a su interacción de control remoto
37	WannaCry	Encryptor	67171	
38	WhatsAppWeb	Goodware	34800	Artefacto Goodware seleccionado debido a que usa cifrado en el envió y recepción de mensajes
39	Winrar	Goodware	53783	Artefacto Goodware seleccionado debido a que usa encripción y cifrado de archivos y/o carpetas
40	Wireshark	Goodware	43594	Artefacto Goodware seleccionado debido a que permite obtener información importante a través de la red mediante archivos pcap
			1836147	**TIEMPO TOTALEN SEGUNDOS**
			510,04	**TIEMPO TOTAL EN HORAS**
			21,25	**TIEMPO TOTAL EN DÍAS**

2.000 Experimentos

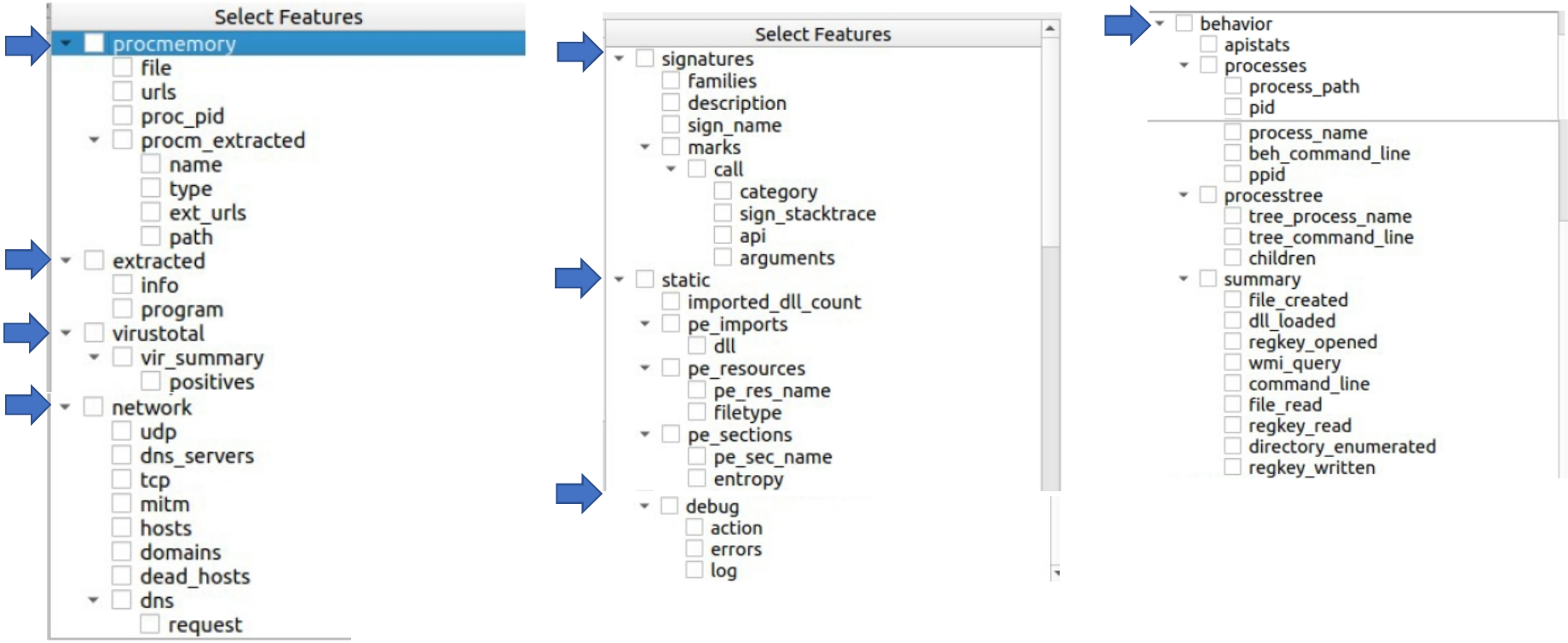
AECI

Generación Automática de Dataset para Modelamiento



AECI

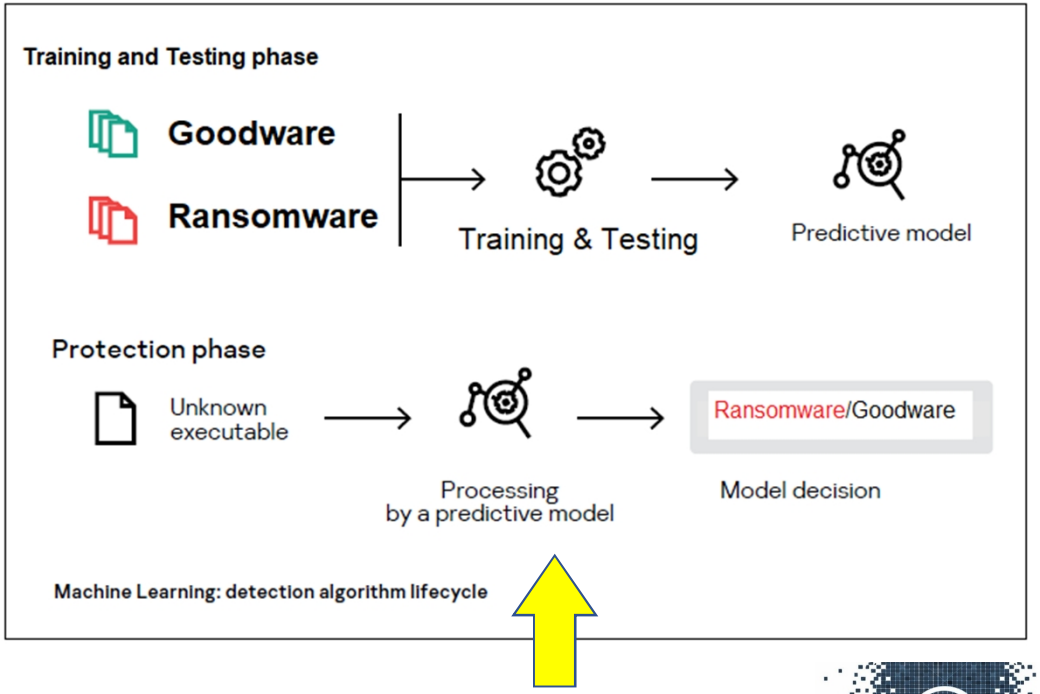
Generación Automática de Dataset para Modelamiento



Selección de hasta 50 Características de cada archivo .JSON

AECI

Nuevos Modelos en Experimentación (Aprendizaje y Testing)



AECI

Detección de Ransomware con Seguridad Cognitiva

Gracias por su Atención.

Preguntas?

mail: juan.herrera@leveltech.com.ec
www.leveltech.com.ec

AECI