ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

Les xifres de programari maliciós el 2023

TLP:WHITE

MARÇ 2024

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	15/03/2024	18/03/2024

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGIA **4**
2. INTRODUCCIÓ **5**
3. TIPUS PRINCIPALS DE PROGRAMARI MALICIÓS DETECTATS DURANT EL 2023 **6**
3.1. Evolució de la seva incidència durant cada trimestre 7
4. FAMÍLIES PRINCIPALS DE PROGRAMARI MALICIÓS DETECTADES EL 2023 **9**
4.1. Evolució de la seva incidència durant cada trimestre 9
5. CARACTERÍSTIQUES DE LES FAMÍLIES PRINCIPALS DE PROGRAMARI MALICIÓS **11**
5.1. Redline Stealer 11
5.1.1 IOC 11
5.2. Remcos 12
5.2.1 IOC 12
5.3. njRAT 13
5.3.1 IOC 14
5.4. Agent Tesla 15
5.4.1 IOC 15
6. CONCLUSIONS **17**
7. CLÀUSULA DE CONFIDENCIALITAT **18**

1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi més bo d'informació delicada (però no classificada) en l'àmbit de la seguretat de la informació.

A través d'aquest esquema, d'una manera àgil i senzilla, s'indica fins on pot circular la informació més enllà del receptor immediat, i aquest ha de consultar l'Agència Nacional de Ciberseguretat d'Andorra quan cal distribuir la informació a tercers.

Codi	Com es fa servir	Com es comparteix
TLP: RED	S'ha de fer servir **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, la reputació o les operacions si es fa servir malament.	Els receptors no han de compartir informació designada com a **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP: AMBER	S'ha de fer servir **TLP:AMBER** quan la informació ha de ser distribuïda de manera limitada, però suposa un risc per a la privacitat, la reputació o les operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com a **TLP:AMBER** només amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per compartir aquesta informació.
TLP: GREEN	S'ha de fer servir **TLP:GREEN** quan la informació és útil per a totes les organitzacions que hi participen, com també amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com a **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP: WHITE	S'ha de fer servir **TLP:WHITE** quan la informació no suposa cap risc de mal ús, conforme a les regles i procediments establerts per a la seva difusió pública.	La informació **TLP:WHITE** pot ser distribuïda sense restriccions, únicament subjecta a controls de copyright.

2. INTRODUCCIÓ

Les xifres sobre l'**impacte del programari maliciós durant el 2023 passat** són preocupants, i és que la seva incidència va augmentar més d'un 11 % i va provocar **més de 6.060 milions d'incidents de ciberseguretat**.

Però el terme programari maliciós fa al·lusió a un concepte molt heterogeni: els programaris maliciosos són molts i molt diversos, i cada un té les seves característiques pròpies i serveix per a un propòsit concret. Per això, mitjançant aquest informe, es farà una anàlisi dels tipus de programaris maliciosos amb una prevalença més gran durant l'any passat.

En aquest document també es podrà trobar un estudi exhaustiu sobre les tendències d'ús dels diferents tipus i famílies de programari maliciós amb les dades recopilades dels incidents registrats. D'aquesta manera es podrà entendre quina tipologia de programaris maliciosos van ser els que es van fer servir més per fer atacs i quines, al contrari, van tenir una presència residual.

D'aquesta manera, l'objectiu final és entendre com funcionen i quin és l'objectiu d'aquells programaris maliciosos que estan involucrats en la majoria dels incidents per, en darrera instància, evitar que puguin comprometre els nostres equips i sistemes.

També s'aportarà informació tècnica, com ara l'IOC, per, en aquells casos en els quals es consideri oportú, es pugui contrastar o actualitzar la informació dels sistemes de detecció.

3. TIPUS PRINCIPALS DE PROGRAMARI MALICIÓS DETECTATS DURANT EL 2023

Per entendre millor quines són les **característiques pròpies de cada un dels diferents tipus de programari maliciós** que conformen el panorama d'amenaces actual, tot seguit, s'enumeren els que van provocar la majoria d'incidents registrats durant l'any passat:

- ***Loader***: és un tipus de programari maliciós **dissenyat per carregar altres programes maliciosos en un sistema compromès**. Es pot fer servir per descarregar o executar altres tipus de programaris maliciosos, com ara troians, programari de segrest o enregistradors de teclats (*keyloggers*).

- **Troià**: s'anomena troià, perquè és un tipus de programari maliciós que actua com un cavall de Troia. És a dir, **aparenta ser programari legítim i el seu objectiu és enganyar els usuaris i guanyar accés als seus sistemes**. Una vegada instal·lat, pot fer una gran varietat d'accions malicioses, com ara robar informació confidencial, instal·lar altres programaris maliciosos i permetre l'accés remot al sistema infectat.

- **RAT (Remote Access Trojan)**: és un tipus de troià dissenyat específicament per **permetre a un atacant controlar remotament el sistema infectat**. Se sol fer servir per espiar els usuaris, robar informació delicada, instal·lar altres tipus de programari maliciós o dur a terme atacs dirigits.

- **Programari de segrest**: es caracteritza per **xifrar els arxius dels sistemes que compromet** per, posteriorment, sol·licitar un rescat a canvi de proporcionar la clau de desxifratge. La finalitat principal del programari de segrest és extorsionar diners als usuaris i organitzacions afectades, i pot causar danys significatius en xifrar dades crítiques i provocar interrupcions en les operacions comercials.

- **Instal·ladors**: són un tipus de programari maliciós que emulen ser un programa legítim d'instal·lació de programari. Quan l'usuari executa l'instal·lador, també **s'instal·la, en segon pla, programari maliciós addicional en el sistema**, sense el coneixement de l'usuari.

- **Lladre d'informació (*stealer, infostealer*)**: estan dissenyats per **robar informació confidencial** dels sistemes infectats, incloses les contrasenyes, les dades de targetes de crèdit, informació bancària i altra informació personal o delicada.

- **Enregistrador de teclat (*keylogger*)**: és un tipus de programari maliciós que **registra i desa les pulsacions de tecles fetes per un usuari en un equip**. D'aquesta manera, l'atacant pot obtenir les seves contrasenyes, números de targetes de crèdit o qualsevol altra informació confidencial que hi introdueixi.

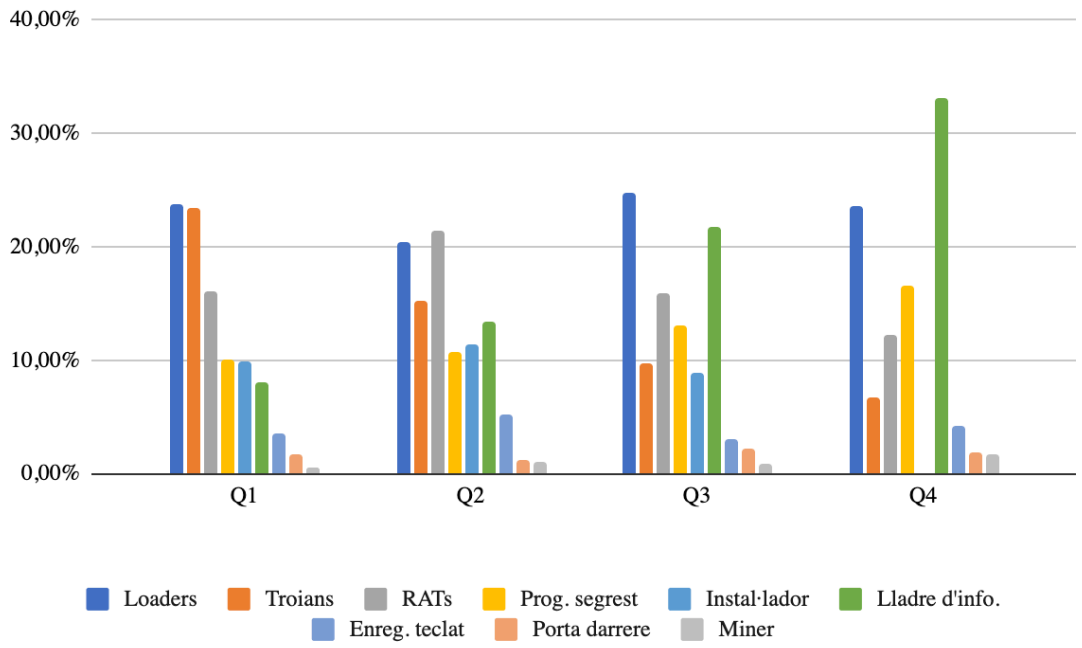
- **Porta del darrere (*backdoor*)**: és una peça de programari maliciós dissenyada per **permetre l'accés no autoritzat a un sistema compromès.** Se solen fer servir per guanyar

persistència en un atac i, d'aquesta manera, mantenir l'accés a aquest sistema fins i tot després que s'hagin pres mesures per limitar el programari maliciós inicial.

- **Miner**: el seu objectiu és **fer servir els recursos d'un sistema compromès per minar criptomonedes de manera il·legítima**. Els miners poden alentir significativament el rendiment del sistema en consumir recursos com la CPU, la memòria i l'energia elèctrica.

3.1. Evolució de la seva incidència durant cada trimestre

En la gràfica següent s'ha representat la relació entre incidents de ciberseguretat i la tipologia de programari maliciós involucrada en cada cas:



Com es pot observar, **durant el primer i tercer trimestre, els *loaders* van ser els tipus de programari maliciós amb un impacte més gran**, amb un 23,81 % i un 24,79 % dels casos analitzats.

En el segon trimestre, els RAT es van situar al capdamunt d'aquesta estadística, cosa que va suposar el 21,46 % del total. I**, en el quart trimestre, i amb un augment de més de 12 punts percentuals, els lladres d'informació van ser el tipus de programari maliciós amb més presència en els successos analitzats**, i van representar el 33,15 % del total.

És interessant observar com la prevalença de diferents tipus de programari maliciós varia al llarg de l'any i com poden experimentar pics en la seva activitat durant determinats trimestres. Això és degut principalment a dues raons: la **capacitat d'adaptabilitat dels atacants i les vulnerabilitats noves que es van descobrint**.

El fet que els lladres d'informació fossin el tipus de programari maliciós més prevalent en el quart trimestre, amb un augment significatiu en la seva incidència, podria indicar una tendència cap a la recol·lecció de dades delicades per part dels atacants. Això podria estar relacionat amb l'augment de la demanda i, per tant, del benefici de la comercialització de dades confidencials en el mercat negre.

La incidència del **programari de segrest es caracteritza perquè es manté molt estable i sense variacions grans al llarg de l'any**. En el primer quadrimestre representa el 9,98 % dels casos, en el segon, el 10,64 %, en el tercer, el 13,12 % i, en el quart, el 16,56 %. És a dir, amb prou feines es produeix una fluctuació d'una mica més del 6 %.

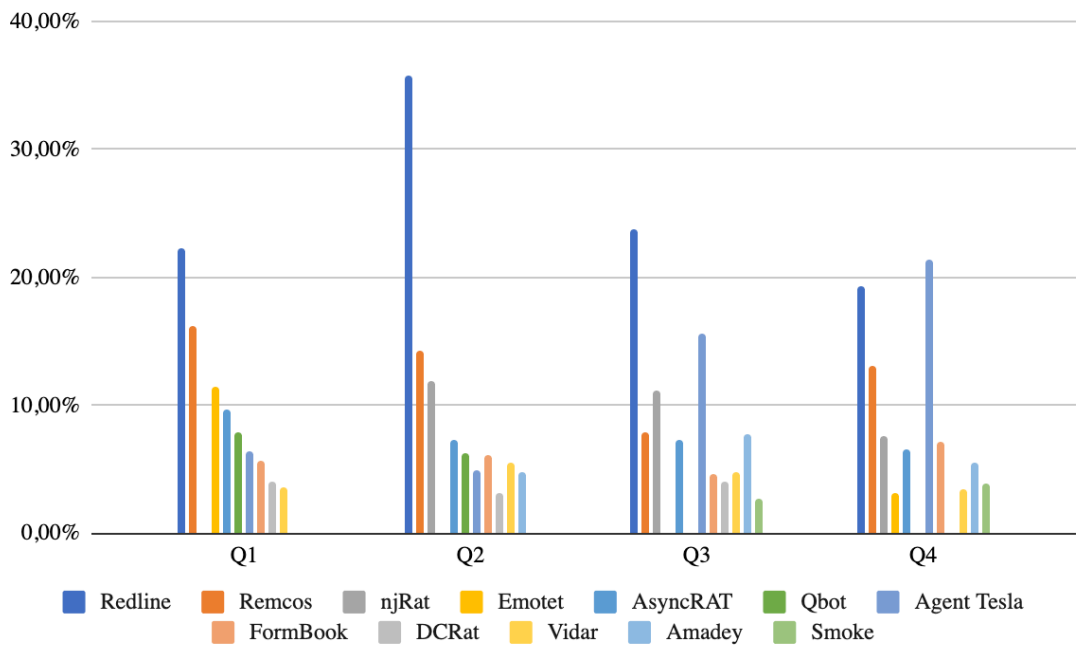
4. FAMÍLIES PRINCIPALS DE PROGRAMARI MALICIÓS DETECTADES EL 2023

En primer lloc, és important entendre la diferència entre tipus de programari maliciós i famílies. A l'apartat anterior hem fet al·lusió als tipus, és a dir, a les categories en què es classifiquen en funció del seu comportament i finalitat.

Quan es parla de famílies de programari maliciós es fa referència als **grups específics de programes maliciosos que comparteixen similituds en el seu codi base, funcionalitat o autoria**. Dintre d'una família de programari maliciós, poden existir variants o versions múltiples del mateix programari maliciós, cada una dissenyada per eludir la detecció d'antivirus i adaptar-se a entorns i sistemes diferents.

4.1. Evolució de la seva incidència durant cada trimestre

A la gràfica següent es recullen les dades sobre les famílies de programari maliciós amb més prevalença durant cada trimestre de l'any passat:



Com es pot observar, el programari maliciós que s'anomena **Redline és el que té més incidència durant els tres primers trimestres de l'any**, i està present en un 22,21 %, 35,77 % i 23,74 % dels casos respectivament.

A l'últim trimestre, tot i que manté una prevalença notable, i se situa per sobre el 19 % de casos, és relegat al segon lloc en detriment del programari maliciós **Agent Tesla que està involucrat en el 21,45 % dels incidents** analitzats. Un programari maliciós que, a més a més,

experimenta la taxa més gran de creixement d'incidència anual atès que en el primer trimestre només estava present en el 6,45 % dels casos estudiats. És a dir, la seva incidència va augmentar en un 15 %.

Atenent els tipus diferents de programari maliciós que pertanyen a cada un de les famílies recollides a la gràfica, es pot establir la correlació que es mostra a la taula següent:

Família de programari maliciós	Tipus de programari maliciós
Redline	Lladre d'informació
Remcos	RAT
njRat	RAT
Emotet	Troià (bancari)
AsyncRAT	RAT
Qbot	Troià
Agent Tesla	Lladre d'informació (programari espia)
FormBook	Lladre d'informació
DCRat	RAT
Vidar	Lladre d'informació
Amadey	Troià
Smoke	Troià

5. CARACTERÍSTIQUES DE LES FAMÍLIES PRINCIPALS DE PROGRAMARI MALICIÓS

Tot seguit, s'analitzaran les característiques principals i s'exposaran els indicadors de compromís propis de cada una de les famílies de programari maliciós amb més prevalença durant el 2023. Redline, Remcos, njRAT i Agent Tesla.

5.1. Redline Stealer

És un programa maliciós de tipus lladre d'informació que està dissenyat per recopilar informació relativa als usuaris i als navegadors dels sistemes que infecta. El seu objectiu principal són les contrasenyes, la informació de les targetes de crèdit, ubicacions, dades d'autocompletar, galetes, informació de programari i, fins i tot, configuracions de maquinari, com la distribució del teclat, la configuració de l'UAC, etc. Redline també pot robar criptomonedes.

Les tècniques de distribució d'aquest programari maliciós no són molt innovadores, tot i que la combinació d'enginyeria social i pesca segueix facilitant que pugui infectar molts sistemes. Alguns dels documents mitjançant els quals es propaga simulen ser del paquet Office, PDF, arxius rar o zip, o executables.

5.1.1 IOC

IP	*Hashes*	Dominis	URL
45.15.156.142	C8983DF41E78AB738B55D9F8F2C1490EEFAE64D5D8DFBAB945B255713094FACC	6.tcp.eu.ngrok.io	http://91.92.254.174:1334/
194.169.175.128	2859A4CA2AFA54E46CEE78C7219FBB6958B4A2835D665FAE68C048B93042A04A	0.tcp.eu.ngrok.io	http://91.198.77.158:4483/
91.92.254.174	4056882CE059EAC4B8351BBC9FD021D7BB44A55088C1F86E4549C0A0F25C8398	4.tcp.ngrok.io	http://185.172.129.234:34244/
45.137.22.252	3876C612BCEDAFE1281A882C80E592354CDCBC8F477D917CC473087F19FFA2EB	4.tcp.eu.ngrok.io	http://185.147.34.93:55615/
135.181.10.212	5594AEE8F2D40CC0A24EE191010F823BE73524E947FFD2B7F6E3E37B18FC9220	7.tcp.eu.ngrok.io	http://93.123.39.68:1334/
91.198.77.158	AF54A35DD3CE3D2584BCC29D858664B3FC7304F0996D7BF07F6AE95E75C5E698	chardhesha.xyz	http://185.222.58.67:55615/
185.172.128.33	2E1FE3C384DBE53288127C5CBFC67E1C000D217C5BA98224C2E52E171736F03B	jalocliche.xyz	http://45.88.186.20:61188/
91.92.241.115	B82336416ABB694B2FEAE39C555E7DDB42FE99DE4F302C8E243F876EA9529F0E	2.tcp.eu.ngrok.io	http://94.156.66.169:1334/
172.86.101.115	ED4FDF645EA14859BFDFC4E61566A7FD0ACAB9FCB42FB4BEF43C032A7AC0A0EA	5.tcp.eu.ngrok.io	http://103.173.227.25:12664/
62.204.41.141	117332FEB820BBD8D10177720DAE9736C7F62DD2FCC5B9518EED427F90AF6524	0.tcp.en.ngrok.io	http://91.92.255.187:1334/
193.161.193.99	5AA518DDB197FFE654BF86DDC59B286E5DE602D02647FBE7B541556504B043A6	galería-gulf.gl.at.ply.gg	http://82.147.85.198:9180/
45.15.156.209	E08DA1E1EE8B136CB4BD34F7F014816D628E2F5212077112A1A4C9BD3A2078CD	ae1.localto.net	http://185.222.58.113:55615/

206.238.199.68	ED226EFF368A0819E2C6011EA218E205C3820E0B20707E14A370519D6C3C028A	6.tcp.ngrok.io	http://185.222.58.115:55615/
194.116.173.25	503DCF7D62D99A266FD74F324E1096E312545429A760B4C29EA94E1D8F57CE98	fhgerbugjreqnhfegrb.top	http://185.222.57.69:55615/
65.0.50.125	C5840E7C7117B70B7F39B73197F32B0475E72A2F3013FF7CCBB3C88F45BA05CC	jamesmillion.xyz	http://185.222.58.239:55615/
93.123.39.68	1CEC72217712823F2227DB94F941D446594250CFB66632C87C879C3BD90D5E9F	exirdonanos.xyz	http://198.244.227.83:6985/
95.217.250.22	AADC1815401D40B4CC922C545A9D571B463AA5C65E3CC811442912294AB59853	denestyenol.xyz	http://178.33.57.150:1334/
65.108.20.226	291F7DA7DDE52E50C3BCDB0125C0E0F6823750C65343A3B3FEDEF56919D588A6	diseño-invitado.at.ply.gg	http://185.222.58.99:55615/
20.218.68.91	1236CB6082AC8E5A19982344F25B020082BD0936E2E5B576F8B3A02703A40DD5	granredking.duckdns.org	http://91.92.243.247:1334/
94.130.56.29	A8F9A453BC6624124834296411BD7D82F2A1168D784034768510D3AFFD83D514	termiya.duckdns.org	http://185.222.58.246:55615/

5.2. Remcos

És un RAT, és a dir, el seu objectiu és permetre que un atacant prengui el control de manera remota d'un equip infectat. Ha estat desenvolupat i es ven per una «empresa» anomenada Breaking Security que, tot i que promet que el programa només està disponible per als qui pretenguin fer-lo servir per a finalitats legals, en realitat és accessible per a qualsevol persona que vulgui llançar un atac potencialment destructiu atès que pot controlar equips amb sistemes operatius Windows.

Està equipat amb un programa criptogràfic que permet que el programari maliciós es pugui ocultar dels antivirus, amb un registrador de tecles i amb un programa d'enviament massiu de correu que es pot fer servir per dur a terme campanyes de distribució i un servei DynDNS amb una connexió client-servidor. És a dir, proporciona els recursos necessaris per crear una xarxa de zombis (*botnet*) funcional.

5.2.1 IOC

IP	*Hashes*	Dominis	URL
107.172.31.19	49E4D4F6AAF967B656487D0D3DC27ECF3812B2D454B85339AE9EA79021BBE0D6	4.tcp.ngrok.io	http://p4-preview.runhosting.com/breakingsec02.co.nf/Remcos/logaccess.php
64.188.20.186	8C71AEB54732D7C292C42820B9B46CD44710C58920BDEE797C8C462B22C3569B	gamemodz.duckdns.org	http://p4-preview.runhosting.com/breakingsec02.co.nf/Remcos/OnlineCheck-v4.php
91.92.241.203	E5DA419608FCF10DD33A0292A84E2453BFE44301D4E2FA28CF9D286A091CB107	4.tcp.eu.ngrok.io	http://p4-preview.runhosting.com/breakingsec02.co.nf/Remcos/login.php
107.175.229.139	A62B6FF9F536F6725A6235B206861F26C6FCF19DD08ED8286DCF90F6D224F3F8	pentester0.accesscam.org	http://p4-preview.runhosting.com/breakingsec02.co.nf/Remcos/upd_free.txt
103.77.243.215	CA3EAA04774A75D793A2E06E566457F10E464D92DD1F193413AD285981773A96	honeypotresearchteam.duckdns.org	

163.123.143.99	18CD3063DCC655B5B9BFFC3692D2E2FBC7199EE08E9C6AB01A1D7A6D6B9CC10E	archived.zapto.org	
74.119.194.217	92E494319D7EE8A055F2FB64BD5F3ED051877289A0948F1E53B485799613B16B	windowsfebupdatenew.duckdns.org	
35.89.75.96	A0EBF0E5B7DDCE607D73F58A9A3A676BC9CC4645BB1918C8DED7D287FD2275B9	febrero27.con-ip.com	
195.54.170.36	2D22CA8B9903FCCF7E1408139E3241B9AF152065EC3810BA1166D2F6B1597EF1	01marzo.con-ip.com	
192.161.184.21	26CAE4CDEEF032AEA2BD4EA1C5B88FBFB876BB3DD35A54076356195969FE3611	sdfsdjhswdbjhd.con-ip.com	
89.249.73.162	7E09B162052FA0F01F2D48609446E1CC66FEA01AFA412D5AEE4CCA9AFA98FE52	windows70393updatemar.duckdns.org	
103.67.163.213	A88132C9EAAAE224C518E6BD900B5708850939DCDB65310E06E513A72424DB07	windows6254uma.duckdns.org	
141.95.84.40	5AF982E3E7BFB72F09C58C942243BDA454F917BC5E0A5B048E579B2C5FAA1085	psolver827.ddns.net	
109.248.150.210	32369A358B4448DDAC71CA827BE83465A2AFC4BE4D64B8693FBC0BAC455B08A1	zoonm.ddns.net	
139.64.172.17	6A5A9F5C3587C3E3CCA2B8154F80137AC89DDD1BF9A3EBD3856FB1CC327553EE	sembe.duckdns.org	
91.223.3.151	4CBD6428426FCDB9A3A2F7BBF32CBBD316D293EAD83A722F9F395BC646110261	marzo6.con-ip.com	
172.96.14.18	199E27CBBA82346D3F8052CCF0F442B59AA2FC3DC5E5FFDD6924B7C6DA42A258	marzo5.con-ip.com	
185.222.58.40	615D9C979A841E23FA80BB7317CFC251C11DFAEF6CC18F5FF2B6C05E6DAFA93B	kdhviusdhiuduidhn.con-ip.com	
104.250.180.178	0C172073C1C65CA9F55B4A5B4286D6A0194E16C496D4696E1333A61B12484264	procesoexitos1.duckdns.org	
172.245.208.5	5FC8AD360FA2674ED65E7ECAEFAC66205EE75FA29D36F78DB61C3CCAEFA8F84C	bendecidos.con-ip.com	

5.3. njRAT

Aquest RAT, que es basa en el marc .NET, té com a particularitat que proporciona als atacants la capacitat d'activar la càmera web, registra pulsacions de tecles i roba les contrasenyes desades als navegadors web, com també a múltiples aplicacions d'escriptori.

A més a més, aquest programari maliciós facilita als pirates informàtics accés a la línia de comandaments de la màquina infectada. D'aquesta manera permet finalitzar processos i executar i manipular arxius de manera remota. A més a més, és capaç de manipular el registre del sistema.

Aquest programari maliciós pot atacar aplicacions de criptomoneders per robar-les. Per exemple, se sap que pot obtenir bitcoins i fins i tot accedir a informació de targetes de crèdit que a vegades es pot emmagatzemar en aplicacions criptogràfiques.

5.3.1 IOC

IP	*Hashes*	Dominis	URL
5.39.43.50	A23153670179DBE891525D06E67A7D6DE6A98EC288230E64322961AD1DBF0A86	4.tcp.eu.ngrok.io	https://pt.textbin.net/download/insdj4bhn2
147.185.221.18	365E7342D6AEC761F8C62AA5326B55CA1A9D2F8EC6BA34BC1476014AB63600E7	ncpanel.hackcrack.io	https://pastes.io/download/g4enqwgps4
94.131.109.101	4CC8CC5BD23BE4B56AE87F5C53DBE2844899AD627A56B2F5F0ED8618CB4FFE5F	startitit2-23969.portmap.host	https://pastebin.com/raw/Hu1K7Y4W
37.75.98.113	45B80BCC484094B4783508B73F18AF348507C1BFF060CDEEEE5FAC8151D42E2A	mexico2020.duckdns.org	https://pastebin.com/raw/VGGi28kN
193.161.193.99	D3DAB8D8F5F7DED7E875BA26CC9CC8296FB99EBBC7E495CEEC4492ED269778D8	seznam.zapto.org	https://pastebin.com/raw/jxx7yjgK
65.0.50.125	24C4F9E8E2112C6712DBAB5667BFD687FD737949B11D385D0E91D219E32159AF	ronymahmoud.casacam.net	https://6ded-177-50-200-148.ngrok-free.app/
94.72.114.95	FB06D35D095B493923BEB34AAC6E25398EF29DFDE3FE76C06F2A0C2E5A926741	wanted-bernard.gl.at.ply.gg	https://pastebin.com/raw/vZM3LPTw
141.95.84.40	9A1B0B047002494A87485F6E598F70EAA2D569F7CF9E351A07715954BEC84264	zakifail.hopto.org	https://pt.textbin.net/download/rcd5ihynxw
89.109.9.59	D8828E904B14533C6AC2BF4B6CDE758FFE06ADB1C83E483A665783938DC4BE5F	windowsupdateservice.mypi.co	https://pastebin.com/raw/UgsiXFgH
147.185.221.17	C6A25C9181BB61EA1925114B42490AF338EF38BDF4BAB8E66D5F80C34B1C1B5D	mistersjsas1.duckdns.org	https://pastebin.com/raw/YKgY3s0H
45.144.166.168	439771DD95416005A5E110BE7AFCF077A91A89FB2086488E4966014598ADFEFA	driver-computational.at.ply.gg	https://pastebin.com/raw/rdmzbeYW
59.21.96.62	0164177547965B708AAA5B0FBD9BFF4C5B033A6F4FA1BC8E569A96D61CE9EE31	7.tcp.eu.ngrok.io	https://pastebin.com/raw/fnugwhmF
94.156.69.231	C31E98B1FB35D34B4944AD1A957C233DDE5E029435FC0C230075037033B12BBA	over-restrictions.gl.at.ply.gg	https://pastebin.com/raw/CmJ80yPc
51.222.15.27	1203FEF12223055B588078484336C8361A6762876F73E524C08DF1D7E46A88C6	zaaptoo.zapto.org	https://pastebin.com/raw/MiKBEm2x
2.56.152.93	3B6074646068CFD2536DF69F95C2B7D45EA1CA196098BEDE73A9DBDCBA8E96E5	junio2023.duckdns.org	https://pastebin.com/raw/LPn410Wj
185.204.1.236	4AF8F255DD229833CA59CF894CE9AD1E3B1685AA6D245356C04E71C2DD69EC60	links-annually.gl.at.ply.gg	https://pastebin.com/raw/GUZjvbiL
31.180.175.236	842A7606A22387E3E980D7D8DC89885462723C3A4DC30EFEF322FD1824D8B7B7	survey-dover.gl.at.ply.gg	https://pastebin.com/raw/q6JvsRJz
85.172.91.115			https://pastebin.com/raw/S1HhZSCU
45.142.182.104			https://pastebin.com/raw/0mKM5dgn
222.186.174.9			https://pastebin.com/raw/TiVt9TvE

5.4. Agent Tesla

Aquest programari espia està dissenyat per robar contrasenyes i existeix des del 2014. Els atacants poden fer servir el programari maliciós per espiar les víctimes, i els permet veure i monitorar qualsevol mena d'acció que facin en un equip infectat.

Se sol programar mitjançant coreus electrònics en campanyes de pesca en les quals s'inclouen arxius adjunts maliciosos que poden simular ser des d'arxius del paquet Office fins a executables.

I precisament és l'augment tan significatiu de la seva presència a les campanyes de correus maliciosos a l'últim trimestre de l'any el que ha provocat que a l'informe es dediqui aquest espai a aquest programari maliciós.

5.4.1 IOC

IP	*Hashes*	Dominis	URL
66.29.151.236	2B0E3076792CBAAD1206B064B9F0DBCDE8B22918D0063233C8D354F25EC5285A	mail.sencan.com.tr	ftp://ftp.acc-engineering.xyz/
198.23.221.13	0C2217B0E413D9557792E23CBE849EAAC0D69C34C42DAD168AB31E989591C8FD	terminal4.veeblehosting.com	https://api.telegram.org/bot6236057808:AAEPjUfD2i1Z2Y6D-v4tJe2o-ZsIOYXQJ0Q/
76.74.235.200	FAF111038426772FA94226A7208E187B25546F2EF131CF9C647888A75C92E43E	mail.bresciagrameen.lk	https://api.telegram.org/bot1338829993:AAGkgJ80sLaIYwBfp79Ps5EtdSP1XH6jBV8/sendDocument
92.38.178.11	DC282458B7F95A4B266A3AD70BC379F56AA3B4EBAA830524D15F6EA61C2C48AA	cp8nl.hyperhost.ua	https://api.telegram.org/bot5843567515:AAEdtJWwcJKNn64U81CKVdG-li_Ejds8raM/
	F5F279DACAAD0EC61AE22C2619BB2FABF308BE3B841CD0311E7B97B16A1A1432	gator3220.hostgator.com	http://www.texlandbd.com/vvs/inc/c874c1a5333207.php
	40C5A3FCC214C1458B2540D2F5BEA07A0CDDD0995DFAFFF23CBDEE8D6F422D2E	mail.melanopharma.com	http://originwealth.ydns.eu/sew/inc/10a5031d37bc79.php
	954C1A6EAA6C9946AEF8DBF957E00B6EB2AB564F564BDE22C4A1C1AF6B7E2C23	mail.okn-makina.com	http://pushkinorigin.ydns.eu/wiz/inc/1d7c50187af637.php
	D52275A861A9396629E78EDCA76C3B3CEC55980115FEADFD0E93CA9C400BBFFA	bezelety.top	https://api.telegram.org/bot5268976687:AAFVn0p7E2gEOnhpsNJOFeUNsuaE1sW24jE/
	8EFB5396B4A7E5FEA2644C844C1AB7E000B8CE9CAFDC1C7172D480731F16C8FC	mail.worlorderbillions.top	ftp://ftp.lemendoza.com/
	AF9373C37EF6F7CEE66F69230DD4BF6F7773153AF373F3485A387C0856EF5DBC	mail.gencoldfire.com	https://api.telegram.org/bot6568247464:AAHsSOES5pRueRqAlbG1bx5hx02y4of2d_Q/
	A4FB4655A4DF0927D8DEF8FA7E8A0F498FFFBDB61858057619482BBBB4F5DE8D	mail.wecaresvc.com	ftp://ftp.onelovehk.com.ng/
	25A1ED4595E074CF8F898B5A0E505809372991F805AEC43F205C254E8D1EC91D	webmail.fashiongroup.pl	ftp://ftp.corpsa.net/
	4D4B2B31829B54D3BD07E43ACF905E6DAB9B872948A4E6DF5509549089A99823	mail.grupobdb.com	ftp://ftp.svetigeorgije.co.rs/
	6B569E9C815E33A762D6514F32C53524A34B104347624AD7CD4C4D591FC9986F	mail.tmf.bg.ac.rs	https://www.ronaldsmith.loan//inc/4e7ada8f7b87bc.php

	F7B800601E3B238161684A6921827DBED9D3F285740028DA7F59E42968FA96CC	mail.fascia-arch.com	https://api.telegram.org/bot5304537825:AAFt7BhY9MUlq_s5TsQbIJu1GotM2jL0xGU/
	4B203E2DC0BA3C82015FE6D72C1EA0874A6A384091927B519062BB51FEB9A567	smtp.pcpatelinfra.com	https://fiores.cl/mail/obrah/inc/dea039b70b5e63.php
	D572D76BC4CBC0096F999A10F7996EFCB014E3E433B05A9A8A25A34ACC280D1A	mail.sturmsgroup.com	https://www.glamourstorepa.com.br/sus2/inc/f858786f876bb9.php
	7590CB175C30E90638D9D0F168ADD1C0CB66D769917EBC3052A9235618A5582B	mail.ivftech.cam	https://www.glamourstorepa.com.br/mail/inc/39dc6fa01a6534.php
	21708C6374A6EB8422C9EAE984BD00A8B8F436A27EF5E1946AAB706FA38F30E1	mail.funworld.co.id	ftp://ftp.mgcpakistan.com/
	21A58C4E3E2C5662146CDE0F2A0E5EE7AA37303C27607C6F9897F9573F89994E	pune.ttspl.in	https://api.telegram.org/bot5556229164:AAG06WuQ2Ibcy5ZKb4lTSDlmionK0lTPWiM/

6. CONCLUSIONS

Després d'haver aprofundit en les característiques pròpies de cada una de les famílies de programari maliciós que han tingut una incidència més gran l'any passat, s'ha pogut comprovar que el mercat de programari maliciós s'ha democratitzat, i ha permès accedir a pràcticament qualsevol usuari a aquestes eines per preus relativament econòmics.

En conseqüència, això ha provocat que les campanyes de distribució es multipliquin, cosa per la qual cal redoblar els esforços per conèixer quins són els mètodes utilitzats per infectar tot aquell equip o sistema susceptible de convertir-se en víctima dels atacants.

A més dels atacs mitjançant programari de segrest, que cal tenir en compte sempre, per la seva gran capacitat de destrucció i el cost tan alt que suposa per a qualsevol organització, és molt important tenir en compte els *loaders*, els troians, els RAT i els lladres d'informació, com ens indiquen les xifres dels registres de l'any passat.

Com també hem vist, el correu electrònic és i continuarà essent el mètode principal de propagació de molts d'aquests programaris maliciosos, per la qual cosa cal redoblar els esforços per no caure en les tàctiques d'enginyeria social impulsades pels ciberdelinqüents amb la intenció d'induir a l'engany per descarregar arxius o fer clic sobre enllaços maliciosos.

7. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació que conté és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones sigui totalment o en part, sense consentiment previ exprés de l'Agència Nacional de Ciberseguretat d'Andorra.