Nro. Alerta:	EC-2022-040	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	07-marzo-2022	**Malware empleado en el conflicto entre Rusia y Ucrania**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Malware
Tipo de incidente: Código Malicioso
Nivel de riesgo: Alta

II. ALERTA

El conflicto entre Rusia y Ucrania se desarrolla tanto en el ámbito físico como en el ámbito digital; estos ataques cibernéticos persistentes entre las dos naciones pueden ser realizados por diferentes actores de amenazas, individuos y organizaciones.

Figura 1. Ilustración asociada a Guerra Cibernética[1]

III. INTRODUCCIÓN

El actual conflicto bélico que se desarrolla entre Rusia y Ucrania también se desenvuelve en el mundo cibernético; algunos expertos le llaman guerras “silenciosas” ya que no existen disparos; sin embargo, el impacto que produce es totalmente significativo.

[1] se define como un ataque cibernético o una serie de ataques dirigidos a un país

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-040	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	07-marzo-2022	**Malware empleado en el conflicto entre Rusia y Ucrania**	V 1.1

En este sentido, entre ambas naciones existen ciberataques como denegación de servicios, malware, campañas masivas de desinformación, entre otros; que son dirigidos a sitios web del Ministerio de Defensa, Ejército y bancos estatales; a fin de provocar pánico y desestabilización. (Tecnología, 2022)

Los ataques de DDoS pueden ejecutarse a través de red de **bots**[2], los mismos inundan los servicios en línea impidiendo el acceso de usuarios legítimos; por otro lado, el uso de malware es ampliamente difundido con el objetivo de destruir información de los distintos sistemas.

IV. VECTOR DE ATAQUE: Remoto

A continuación, se mencionan los diferentes ataques persistentes:

Grupo Ransomware Conti

A través de un comunicado este grupo manifestó su apoyo al gobierno ruso y conforme a informes de investigación se identificó a Ransom.Win32.CONTI.SMYXBLD.

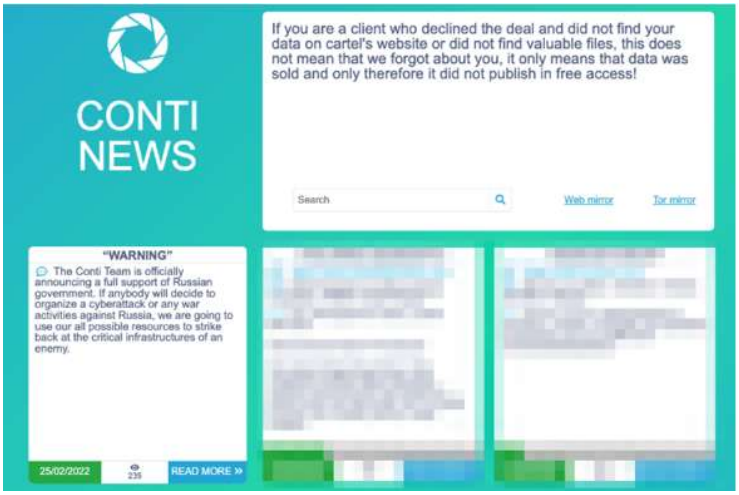


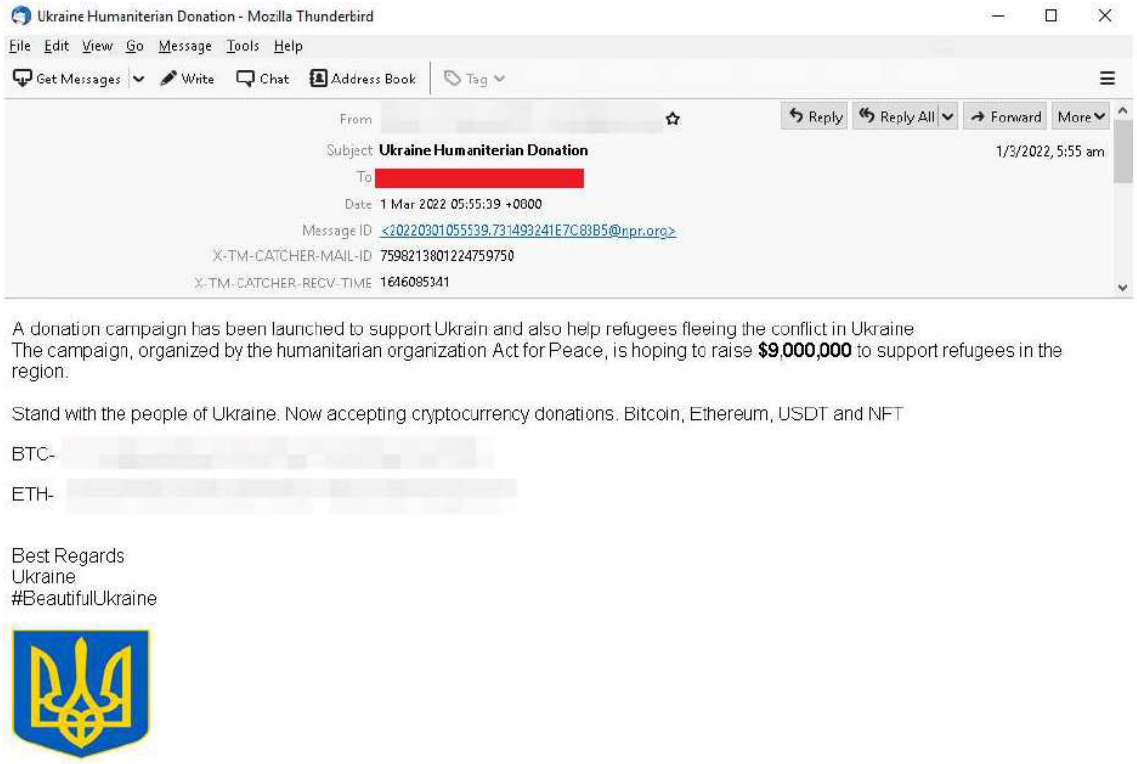
Figura 2. Ilustración asociada al comunicado del Grupo Ransomware Conti
Fuente: TREND MICRO

[2] Herramienta digital que se usa para realizar tareas repetitivas, predefinidas y automatizadas.

Nro. Alerta:	EC-2022-040	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	07-marzo-2022	**Malware empleado en el conflicto entre Rusia y Ucrania**	V 1.1

SPAM relacionados con Ucrania

Otra manera de ataque que se encuentra ampliamente difundido durante este conflicto es el uso de correos electrónicos no deseados. A continuación, se indican mensajes relacionados.



Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-040	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	07-marzo-2022	**Malware empleado en el conflicto entre Rusia y Ucrania**	V 1.1

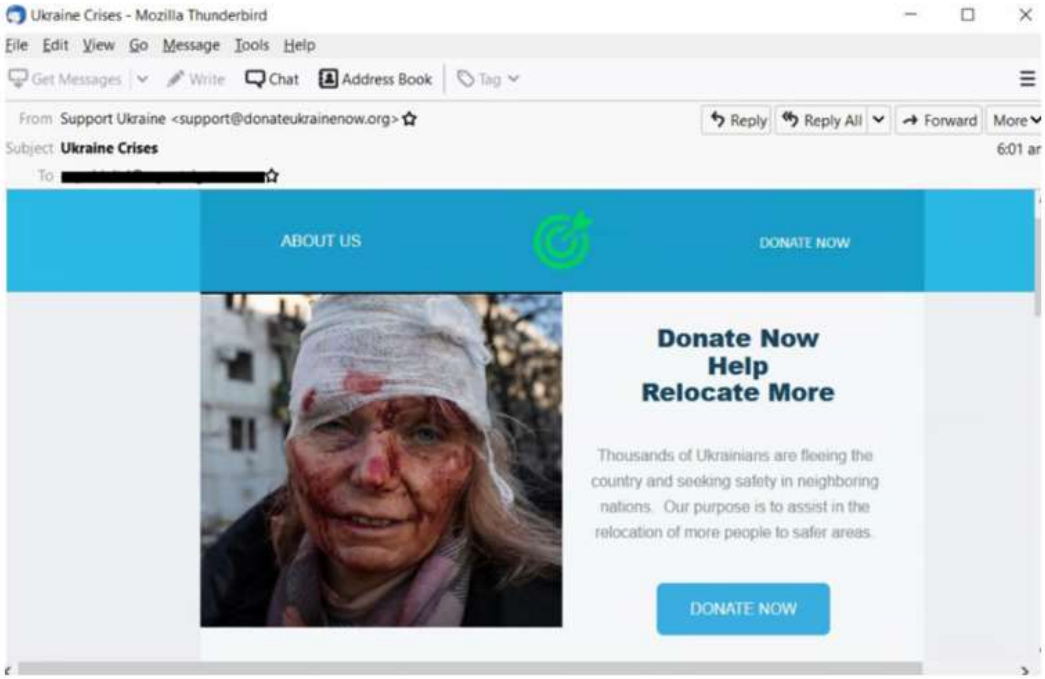


Figura 3. SPAM relacionado con Ucrania.
Fuente: TREND MICRO

WhisperGate

El despliegue de ese primer malware se ocultó bajo la apariencia de un brote de ransomware falso y durante una serie de desfiguraciones coordinadas de sitios web del gobierno ucraniano. WhisperGate descarga y ejecuta una carga útil adicional desde el servidor C&C construido en Discord; así mismo, descarga **WhisperKill** que es el malware encargado de destruir archivos con extensiones específicas. Se estima que alrededor de 70 sitios web de ucrania fueron atacados.

Nro. Alerta:	EC-2022-040	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	07-marzo-2022	**Malware empleado en el conflicto entre Rusia y Ucrania**	V 1.1

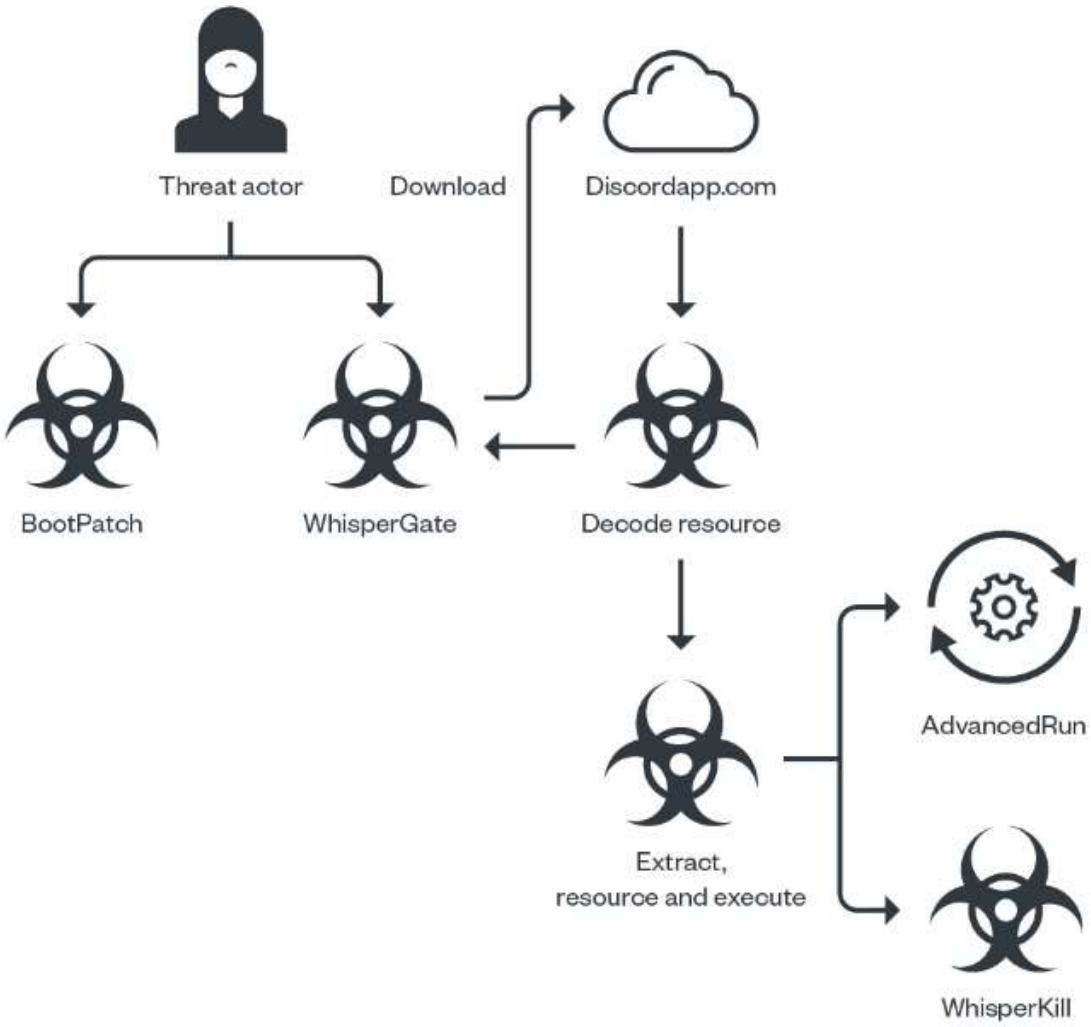


Figura 4. Cadena de infección de Malware WhisperGate
Fuente: TREND MICRO

Nro. Alerta:	EC-2022-040	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	07-marzo-2022	**Malware empleado en el conflicto entre Rusia y Ucrania**	V 1.1

SaintBot

Este Malware está diseñado para estar inactivo cuando el LCID (Identificador de código de idioma) del dispositivo infectado está en Rusia, Ucrania, Bielorrusia, Armenia, Kazajstán o Moldavia. Este ataque empieza a través del phishing enviados supuestamente por el Servicio Nacional de Salud de Ucrania, incluyendo un documento adjunto y dos archivos de acceso directo; uno de estos archivos contiene el malware OutSteel.

```
BOOL ws_check_locale()
{
  int v1; // [esp+0h] [ebp-4h] BYREF

  v1 = 0;
  return ntdll_NtQueryDefaultLocale(0, &v1) >= 0
      && (v1 == 1049 || v1 == 1058 || v1 == 1059 || v1 == 1067 || v1 == 1087 || v1 == 2072 || v1 == 2073);
}
```

Figura 5. Instrucción para verificar LCID.
Fuente: TREND MICRO

Gamaredon

Este actor de amenaza se distribuye a través de correos electrónicos de phishing inyectando una plantilla remota que incluye una macro maliciosa.

La macro decodificada e insertada suelta VBScript en **%APPDATA%:define (ADS),** y luego se registra una tarea programada para ejecutar el script. Este script descarga y ejecuta una carga útil adicional desde el servidor C&C

Nro. Alerta:	EC-2022-040	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	07-marzo-2022	**Malware empleado en el conflicto entre Rusia y Ucrania**	V 1.1

```
Set jamyKxKU = CreateObject("Word.Application")

hampereLwLVRB = "developmentRAmXo"
jamyKxKU.Visible = False

End If
Set counselmEpMH = jamyKxKU.Documents.Add

breakfastjTjxrtE = shipIlenoOu
Set perverseNfR = counselmEpMH
perverseNfR.VBProject.VBComponents.Item(1).CodeModule.AddFromString breakfastjTjxrtE

indeedmUm = "frayUSrkK"
Set flawnvtQZhD = perverseNfR
flawnvtQZhD.Application.Run "VZ01"

quenchByxTIjo = "constraintsntpWtht"
Set darknessNOBZPSH = flawnvtQZhD
darknessNOBZPSH.Close SaveChanges:=wdDoNotSaveChanges

propasoKc = "sewSGRJkec"
jamyKxKU.Quit
```

Figura 6. Muestra de Código malicioso
Fuente: TREND MICRO

HermeticWiper

Es un malware más sofisticado con la capacidad de destruir el MBR y los archivos en las unidades; también conocido como FoxBlade.

Nro. Alerta:	EC-2022-040	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	07-marzo-2022	**Malware empleado en el conflicto entre Rusia y Ucrania**	V 1.1

En la siguiente tabla se indican una breve descripción de los ataques mencionados anteriormente.

Ítem	Descripción	Detalle
1	Grupo Ransomware Conti	Ransom.Win32.CONTI.SMYXBLD
2	SPAM	hxxps://netizenati[.]org savethekidsukraine[.]com
3	WhisperGate	Malware que modifica el contenido del sitio Web, se estima que atacó alrededor de 70 sitios web ucranianos.
4	SaintBot	hxxp://8003659902[.]espacio/wp-adm/gate.php hxxp://smm2021[.]net/wp-adm/gate.php hxxp://8003659902[.]site/wp-adm/gate.php
5	Gamaredon	hxxp://<dirección IP de deep.deserts.coagula[.]online>/barefooted.cfg<hora actual + 1 segundo> (por ejemplo, hxxp://10.172.0[.]3/barefooted.cfg2022/02/03 %2020:49:31
6	HermeticWiper	Dirigido a empresas de sector energético, marítimo, de transportes e infraestructuras críticas de Ucrania

Tabla 1. IOC asociados a RuRat.
Fuente: Cluster25

V. INDICADORES DE COMPROMISO

A continuación, se mencionan los indicadores de compromiso asociados a los ciberataques.

Descripción	Nombre del archivo
RANSOMWARE CONTI	
Ransom.Win32.CONTI.SMYXBLD	3a81355ccfd6d3846fa435b5893ea5cd18e6c9fa
	a803a4b305415b66f22ed29d08017c286b8cb9ef
	b9505c86dd3ae120c0be1201e51af44de4266b36
	655269c264f7b044d8f406cd980fc00c3b8e21ca
	38cd341de09c7d393adf93596b691e7237d0a2e7
	6c7b35e36830c1cc613fb08280ee25e5fbba9937
	5bf5551cee1635709598c90836733550727245ba
	5f27447dcc66c1c4152e23decb47f82c32883080
	911c16d41f49198482aa4d75054cb0e10b07d68c

Nro. Alerta:	EC-2022-040	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	07-marzo-2022	**Malware empleado en el conflicto entre Rusia y Ucrania**	V 1.1

Descripción	Nombre del archivo
SPAM	
TrojanSpy.Win32.AVEMARIA.AYAD| TROJ.Win32.TRX.XXPE50FFF053	f6294b2acf0f15453697f16597de734da8a9d92f
WHISPERGATE	
Trojan.Win32.WHISPERGATE.YXCAQ | TROJ.Win32.TRX.XXPE50FFF053	189166d382c73c242ba45889d57980548d4ba37e
Trojan.MSIL.WHISPERGATE.YXCAQ| TSPY.Win32.TRX.XXPE50FFF053	16525cb2fd86dce842107eb1ba6174b23f188537
Trojan.MSIL.WHISPERGATE.YXCAQ	b2d863fc444b99c479859ad7f012b840f896172e
Trojan.Win32.FRS.VSNW11A22	4c5006cee3e3f7147df37cd03775bfd48e572ca5
Trojan.MSIL.WHISPERGATE.YXCAQ	82d29b52e35e7938e7ee610c04ea9daaf5e08e90
Trojan.Win32.WHISPERGATE.YXCAX	a67205dc84ec29eb71bb259b19c1a1783865c0fc
Trojan.MSIL.WHISPERGATE.YXCBU	97aa0b096abc89d403a2176079fb77be990a4011
SainBot	
Backdoor.Win32.SAINTBO T.A	e8207e8c31a8613112223d126d4f12e7a5f8caf4acaa f40834302ce49f37cc9c
Trojan.MSIL.SAINTALL.A	75f728fa692347e096386acd19a5da9b02dca372b66 918be7171c522d9c6b42d
Gamaredon	
TROJ_FRS.VSNTB322	cbc7f2afe334bc160b741dde2e857ff26e01925744b9f 0668a826aa4a1437ab8
TROJ_FRS.VSNTB322	a82cb2076b7274179d5f7246f8db274eda47a893928 75b3c700f2fa15d70ab2e
Trojan.W97M.TEMPLINJECTOR.ZGJB	839170c51d75bd1dc77f17b957846ace0caa19a83de 837277d7294a47e5023b3
Trojan.W97M.DULLDOWN.ZGJB	bdb4f98bf2bed83b09278bcf7b85771688fb1292612d 6c82ad0eb8d7e3256fa1
TROJ_FRS.VSNTB322	cbc7f2afe334bc160b741dde2e857ff26e01925744b9f 0668a826aa4a1437ab8
Trojan.X97M.CVE20170199.YXCBP	edecec2c413770fa929937c04ecf889e5c58d562c6e0 8ef0bfcd65ce482d397c
Trojan.W97M.TEMPLINJECTOR.ZGJB	6f21dde5cf5394eebf779451d45494dfeb22c2eebbb4 af1aa3f779724dadf8af
Trojan.W97M.TEMPLINJECTOR.ZGJB	aa07ab7dba1aeb41c57bcdcbca54cefb85afb6f8927d 33bf88aef5c19878ba92

Nro. Alerta:	EC-2022-040	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	07-marzo-2022	**Malware empleado en el conflicto entre Rusia y Ucrania**	V 1.1

Descripción	Nombre del archivo
Trojan.X97M.CVE20170199.YXCBP	8831eb86996d4778be526a6fd281c98d624b155940a ae463b45dda1c5f979f1c
Trojan.W97M.TEMPLINJECTOR.ZGJB	3590dd881d094b020fe4b93bb6894e768b878ebcda7 f03589da6671db2c652e5
Trojan.W97M.TEMPLINJECTOR.ZGJB	420960a10e3f3730ab124bfefceedc032ef06c7b38fa0 14b2b59462365a5f08d
URL	deep-pondering[.]gortomalo[.]ru hxxp://185.46[.]10.45/wordpress.html hxxp://185.46[.]10.45/counter.html deep-six[.]gortomalo[.]ru hxxp://185.46[.]10.45/set.lgo/deerfood3 hxxp://185.46[.]10.45/currently/credit/m4v hxxp://185.46[.]10.45/set.lgo/deerfood223 hxxp://5.252.178.184 5.252.178[.]184:33163 deprive.lotorgas[.]ru hxxp://5.252.178.188 2.59.36[.]204 5.252.178[.]183 ambulance[.]globe24[.]koparas[.]ru ambulance[.]globe90[.]koparas[.]ru configolders4_config4[.]vivaldar[.]ru counteract[.]end22[.]kassanfo[.]ru countless[.]intercept37[.]freebsdo[.]ru enforce[.]shoes34[.]linuxo[.]ru naturally[.]stopped100[.]kilotora[.]ru necessity[.]amateur100[.]pitroksa[.]ru koparas[.]ru loralis[.]ru pitroksa[.]ru aaa.loralis[.]ru aaa.koparas[.]ru aaa.pitroksa[.]ru gloomily67.golitus[.]ru interference20.holotras[.]ru 2.59.36.194
HermeticWiper	
Trojan.Win32.KILLDISK.SMYECBW | TROJ.Win32.TRX.XXPE50FFF053E0002	61b25d11392172e587d8da3045812a66c3385451
Trojan.Win32.KILLDISK.SMYECBW |	912342f1c840a42f6b74132f8a7c4ffe7d40fb77

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-040	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	07-marzo-2022	**Malware empleado en el conflicto entre Rusia y Ucrania**	V 1.1

Descripción	Nombre del archivo
TROJ.Win32.TRX.XXPE50FFF053E0003	
Trojan.Win32.KILLDISK.SMYECBW | TROJ.Win32.TRX.XXPE50FFF053E0002	9518e4ae0862ae871cf9fb634b50b07c66a2c379
Trojan.Win32.KILLDISK.SMYECBW | TROJ.Win32.TRX.XXPE50FFF053E0003	d9a3596af0463797df4ff25b7999184946e3bfa2
Trojan.Win32.KILLDISK.SMYECBW | TROJ.Win32.TRX.XXPE50FFF053E0004	0d8cc992f279ec45e8b8dfd05a700ff1f0437f29
OutSteel	
TrojanSpy.MSIL.OUTSTEEL.YMCBB	7ee8cfde9e4c718af6783ddd8341d63c4919851ba64 18b599b2f3c2ac8d70a32
Trojan.Win32.FRS.VSNW14B22	320d091b3f8de8688ce3b45cdda64a451ea6c22da1fc ea60fe31101eb6f0f6c2
Clipbanker Malware	
TrojanSpy.Win32.CLIPBANKER.TH COABB	0fbd7abc2755ccc4d853d06ca7ad8562c5c12b40
TROJ_FRS.0NA104BP22	728da6dea7be8c4249c40bb45ead9a4885257d72d1 30db3caa0e19c108041760
TROJ_FRS.0NA104BP22	738c3dbc72b2edcb0e90eda5e235d4398a42326099 954a20a9691e02bf1f8ab0
URL	hxxp://179.43.175[.]171/qelh/CL.exe hxxp://179.43.175[.]171/qelh/png.hta
Stormous Ransomware	
Ransom.PHP.STORMOUS.YXCCBT	96ba3ba94db07e895090cdaca701a922523649cf6d6 801b358c5ff62416be9fa
HTML.STORMOUS.YXCCBT.no te	b7863120606168b3731395d9850bbf25661d05c6e09 4c032fc486e15daeb5666

Tabla 2. IOC asociados a ataques entre Rusia y Ucrania
Fuente: Trend Micro

VI. RECOMENDACIONES:

Los ataques dirigidos entre Rusia y Ucrania pueden extenderse repentinamente a otros países y los objetivos desprevenidos pueden verse afectos; razón por la cual, el EcuCert recomienda a su comunidad objetivo:

Nro. Alerta:	EC-2022-040	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	07-marzo-2022	**Malware empleado en el conflicto entre Rusia y Ucrania**	V 1.1

- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución.
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Tener actualizado y utilizar, un software anti-virus.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.
- Implementar un plan de respuesta a emergencias de la Organización/Institución.

VII. REFERENCIAS:

Cimpanu, C. (23 de 02 de 2022). *The Record* . Obtenido de The Record : https://therecord.media/second-data-wiper-attack-hits-ukraine-computer-networks/

Micro, T. (03 de 03 de 2022). *Trend Micro*. Obtenido de Trend Micro: https://www.trendmicro.com/pl_pl/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html

Tecnología, E. P. (26 de 02 de 2022). *El País*. Obtenido de El País: https://elpais.com/tecnologia/2022-02-26/la-ciberguerra-de-rusia-contra-ucrania-nunca-ha-acabado.html

TrendMicro. (03 de 03 de 2022). *TrendMicro*. Obtenido de TrendMicro: https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict/IOC%20Resource%20for%20Russia-Ukraine%20Conflict-Related%20Cyberattacks-03042022.pdf