CYBER
THREAT
ANALYSIS
CHINA

Recorded Future®

By Insikt Group®

December 23, 2022

RedDelta Targets European Government Organizations and Continues to Iterate Custom PlugX Variant

This report details recent activity conducted by the likely Chinese state-sponsored threat activity group RedDelta. The activity was identified through a combination of large-scale automated network traffic analytics and expert analysis. This report will be of most interest to individuals and organizations with strategic and operational intelligence requirements relating to Chinese cyber threat activity, as well as network defenders in government organizations within Southeast Asia and Europe.

Executive Summary

Recorded Future's Insikt Group continues to track activity we attribute to the likely Chinese state-sponsored threat activity group RedDelta targeting organizations within Europe and Southeast Asia using a customized variant of the PlugX backdoor. Since at least 2019, RedDelta has been consistently active within Southeast Asia, particularly in Myanmar and Vietnam, but has also routinely adapted its targeting in response to global geopolitical events. This is historically evident through the group's targeting of the Vatican and other Catholic organizations in the lead-up to 2021 talks between Chinese Communist Party (CCP) and Vatican officials [1,2], as well as throughout 2022 through the group's shift towards increased targeting of European government and diplomatic entities following Russia's invasion of Ukraine.

During the 3-month period from September through November 2022, RedDelta has regularly used an infection chain employing malicious shortcut (LNK) files, which trigger a dynamic-link library (DLL) search-order-hijacking execution chain to load consistently updated PlugX versions. Throughout this period, the group repeatedly employed decoy documents specific to government and migration policy within Europe. Of note, we identified a European government department focused on trade communicating with RedDelta command-and-control (C2) infrastructure in early August 2022. This activity commenced on the same day that a RedDelta PlugX sample using this C2 infrastructure and featuring an EU trade-themed decoy document surfaced on public malware repositories. We also identified additional probable victim entities within Myanmar and Vietnam regularly communicating with RedDelta C2 infrastructure.

RedDelta closely overlaps with public industry reporting under the aliases BRONZE PRESIDENT, Mustang Panda, TA416, Red Lich, and HoneyMyte.

Key Judgments

- RedDelta has consistently conducted long-term cyber-espionage campaigns in line with the strategic interests of the Chinese government, including historical targeting of government and public sector organizations across Asia and Europe as well as overseas organizations associated with minority groups within mainland China such as Tibetan and Catholic Church-related entities.
- Despite the volume of public reporting on the group's activity, RedDelta employs a high operational tempo relative to other state-sponsored actors. The group also maintains a rapid pace of development for its flagship backdoor (remote access trojan [RAT]), a variant of the long-running backdoor PlugX that is heavily customized for anti-analysis for detection evasion.
- In November 2022, RedDelta actors shifted from using archive files to using malicious optical disc image (ISO) files containing a simplified shortcut (LNK) file for delivery of an updated PlugX payload.

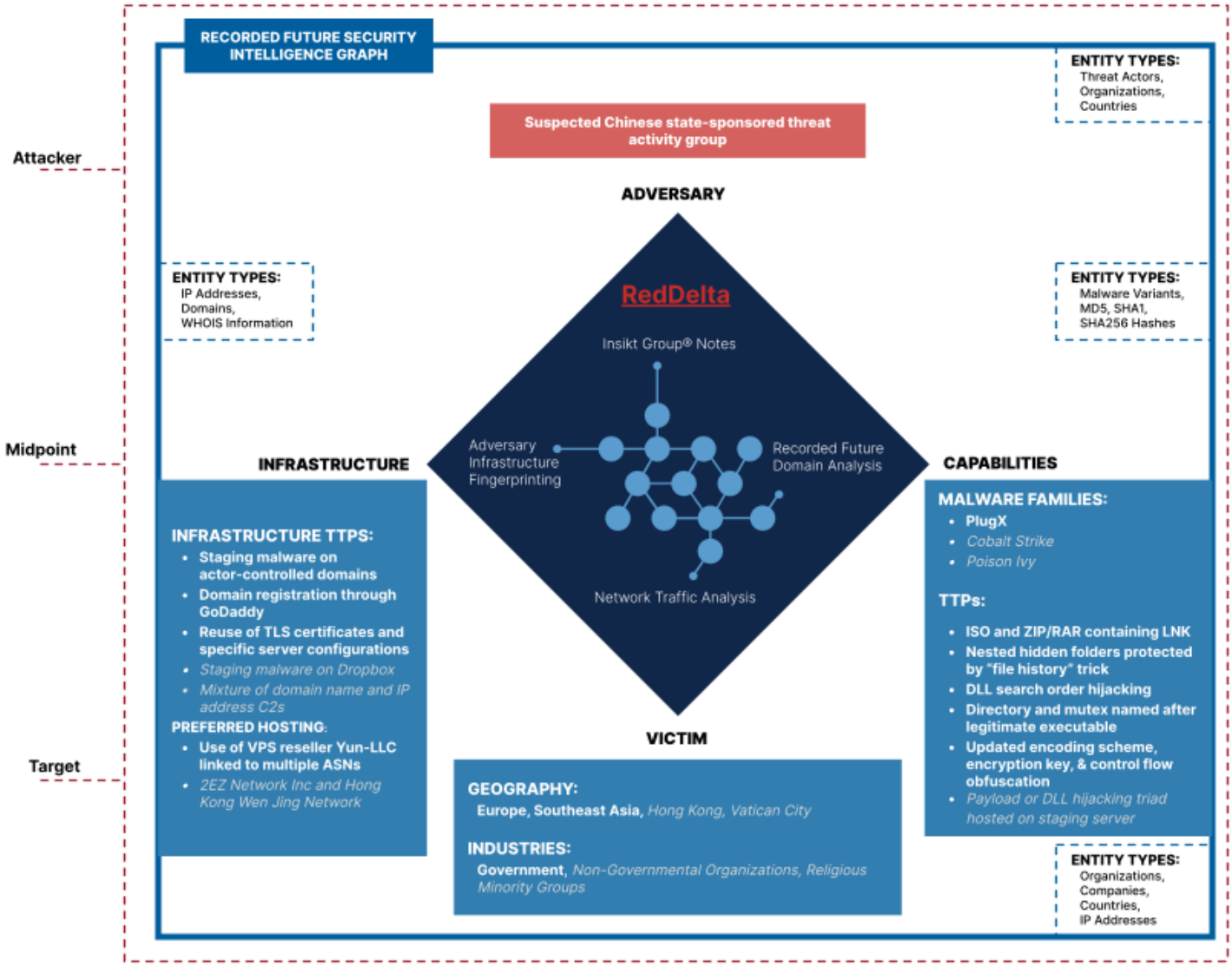


Figure 1: *High-level RedDelta TTPs and Recorded Future data-sourcing graphic; historically reported TTPs are shown in gray [1,2] (Source: Recorded Future)*

Background

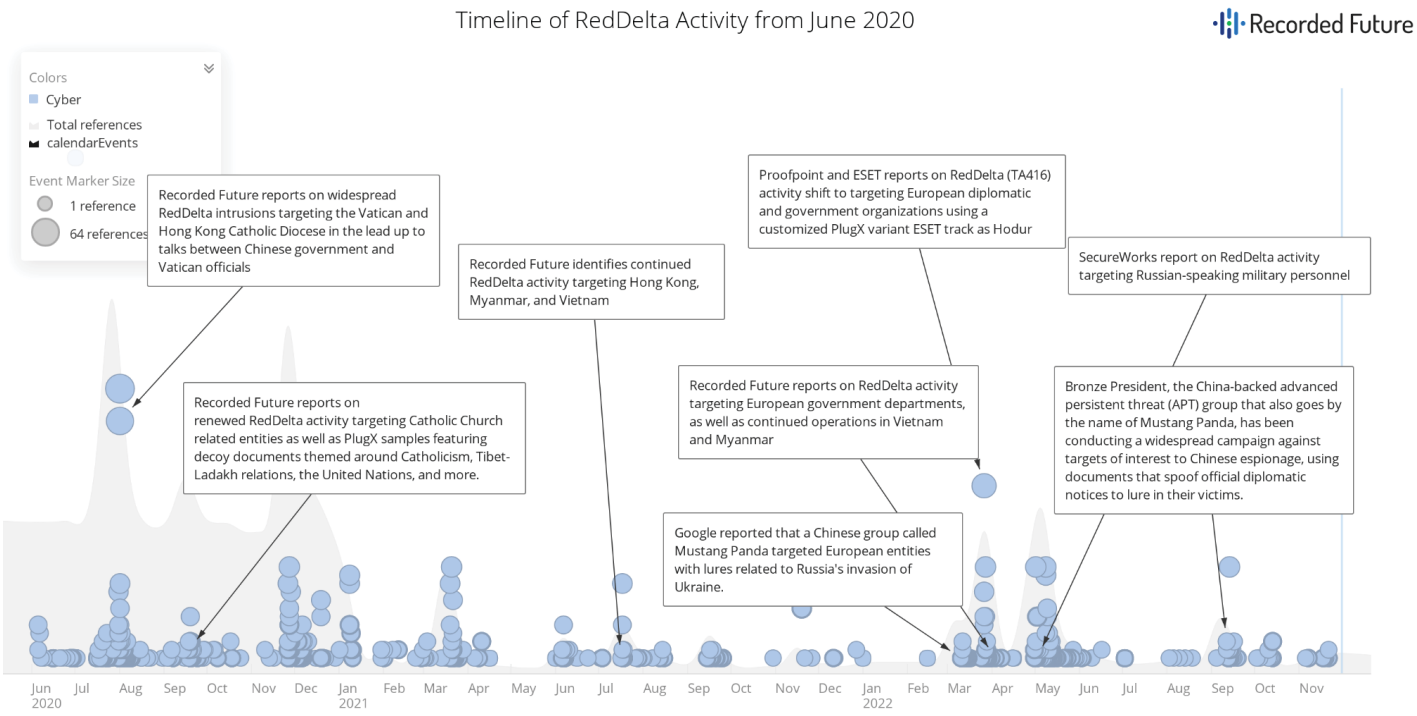


Figure 2: *Timeline of RedDelta activity from June 2020 to November 2022 (Source: Recorded Future)*

In mid-2020, we published research identifying RedDelta intrusions targeting several Catholic Church-related organizations, including the Vatican and the Catholic Diocese of Hong Kong. This activity took place in the lead-up to negotiations between Chinese Communist Party (CCP) and Vatican officials. These findings were also later corroborated by NortonLifeLock. In addition to the targeting of entities related to the Catholic Church, we also identified RedDelta network intrusions affecting law enforcement and government entities in India, a government organization in Indonesia, and other targets across Myanmar, Hong Kong, and Australia. In this activity the group used multiple malware variants including a customized PlugX variant, Cobalt Strike, and Poison Ivy.

Shortly after the publication disclosing activity targeting the Vatican, we identified renewed RedDelta activity again targeting Catholic Church-related organizations as well as an entity associated with the Tibetan community-in-exile. Other high-profile intrusions conducted by RedDelta in 2020 include the compromise of the African Union.

Throughout 2021, we observed continued RedDelta activity targeting government organizations in Indonesia, Myanmar, and Vietnam. In late 2021 and early 2022, RedDelta targeting shifted back toward Europe and the group began using decoy documents themed around escalating tensions between Russia and Ukraine, and eventually around the war itself, as disclosed within customer-facing Insikt Group research and public reporting by Proofpoint, Secureworks, and ESET.

Threat/Technical Analysis

Infrastructure Analysis

In March 2022, we and other researchers reported on renewed RedDelta activity targeting European government and diplomatic organizations, in many cases using lure documents centered on the war in Ukraine [1, 2, 3]. Since this reporting, we have continued to observe similar activity targeting Europe, some of which has been covered through Secureworks reporting.

In contrast to historical activity, RedDelta has largely moved away from use of domain names for C2 infrastructure toward hardcoded actor-controlled virtual private server (VPS) IP addresses. Since March 2022, the group has used a wide variety of autonomous systems (ASs), with a particular preference for the following autonomous system numbers (ASNs):

- GreenFloid — AS204957
- Aptum Technologies — AS13768
- Input Output Flood LLC — AS53755
- QuadraNet — AS8100
- XNNET — AS6134

In many cases, the actor's operational infrastructure on the above ASNs was likely purchased through a China-based VPS reseller called Yun-LLC (vm[.]sg). We have also observed consistent use of specific server responses and multiple reused TLS certificates since March 2022, some of which was referenced in recent Blackberry reporting.

Victimology

We observed likely victims in Vietnam and Myanmar communicating with RedDelta C2 infrastructure throughout 2022, which aligns with the typical historical targeting of the group. We also identified multiple IP addresses associated with a European government department focused on trade regularly communicating with the RedDelta C2 IP address 64.34.205[.]178 on August 9, 2022. On this date, we also observed a RedDelta PlugX phishing campaign featuring an EU trade-themed decoy document using this C2, which surfaced on public malware repositories. We have not observed any further evidence of compromise for this organization since this date.

Malware Analysis

Initial Infection Vector — August to October 2022

The infection vector used from August to October 2022 remained largely unchanged from recent Secureworks and BlackBerry reporting covering RedDelta activity (tracked as BRONZE PRESIDENT by Secureworks researchers). In each case, an archive file is delivered to the targeted user, likely via spearphishing, which contains a Windows shortcut (LNK) file disguised using a double extension (such as .doc.lnk) and a Microsoft Word icon. The archive also features a series of nested hidden folders that contain 3 files used within a DLL search-order-hijacking triad: a legitimate binary, a malicious DLL loader, and an encrypted PlugX payload that is ultimately loaded into memory. Upon execution of the shortcut file, this executes the legitimate binary vulnerable to DLL search order hijacking and also displays a decoy document to the victim.

The observed RedDelta LNK files during this timeframe were created on a system with the hostname `desktop-n2v1smh`, which was previously noted in earlier LNK files used by the group. In each case, the LNK file contains a similar argument to the example shown in **Figure 5** in order to run the legitimate executable and start the DLL search-order-hijacking chain:

```
   "_\___\_\___\______\_____\__\test11.
bpu||(forfiles /^P %USERPROFILE%\ /S /^M
"Political Guidance for the new EU approach
towards Russia.rar" /C "cmd /c (c:\progra~1\7-
Zip\7z x -y -aoa @path||c:\progra~2\7-Zip\7z x
-y -aoa @path||c:\progra~1\winrar\winrar x -id
-o+ @path||c:\progra~2\winrar\winrar x -id -o+ @
path)&&_\___\_\___\______\_____\__\test11.bpu")"
```

Figure 5: *Example of command run by LNK file to trigger DLL search-order-hijacking chain (Source: Recorded Future)*

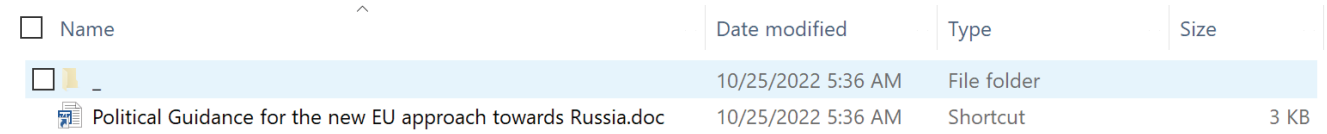


Figure 3: *LNK file masquerading as a .doc file due to use of a double extension and Microsoft Word icon (Source: Recorded Future)*

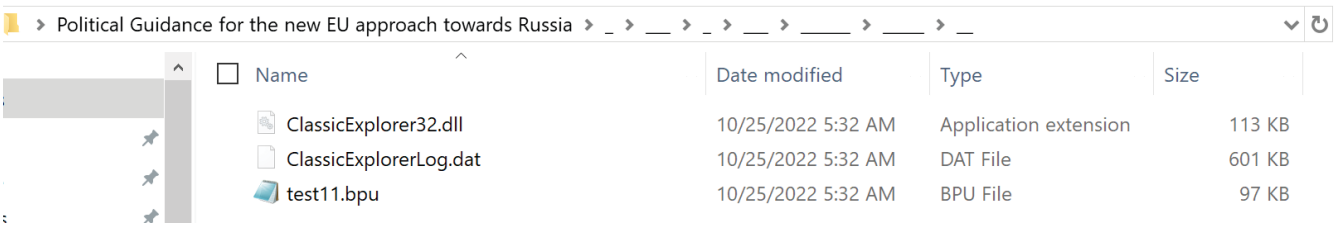


Figure 4: *Nested hidden folder containing a legitimate executable (ClassicExplorerSettings.exe renamed as test.bpu), malicious DLL loader (ClassicExplorer32.dll), and encrypted payload (ClassicExplorerLog.dat) (Source: Recorded Future)*

Initial Infection Vector - November 2022

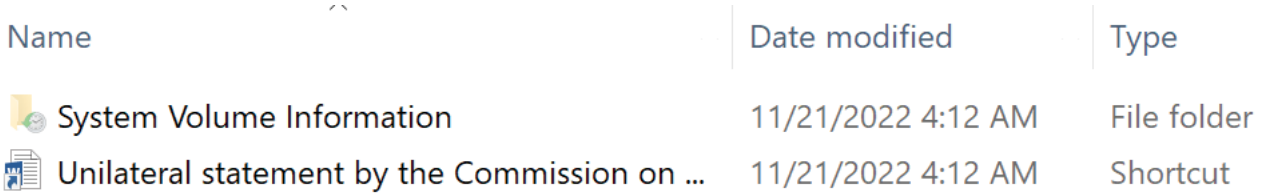


Figure 6: *Contents of ISO file "Unilateral statement by the Commission on migration.iso" used in November 2022 (Source: Recorded Future)*

In November 2022, we identified new RedDelta activity using a slightly altered infection chain. In this case an ISO file titled "*Unilateral statement by the Commission on migration.iso*" was served through the actor-controlled domain microsite-manager[.]com, which was hosted on IP address 5.34.182[.]68 at the time of analysis. This IP address also concurrently hosted a probable additional RedDelta domain, mashupdatabase[.]com, which was registered through GoDaddy at the same time as microsite-manager[.]com.

Similar to previously described activity, the ISO contained an LNK file and nested hidden folders titled `System Volume Information` containing the DLL search-order-hijacking triad, as shown in **Figure 6**. Notably, in this case the `System Volume Information` folder also contains a `desktop.ini` file featuring a Class ID (CLSID) Key shortcut `{F6B6E965-E9B2-444B-9286-10C9152EDBC5}`, which corresponds to the File History utility in Microsoft Windows. Interestingly, this folder is interpreted by File Explorer as a legitimate shortcut to File History, and redirects the user to this utility rather than displaying the true malicious contents of the folder that are executed using the LNK file.

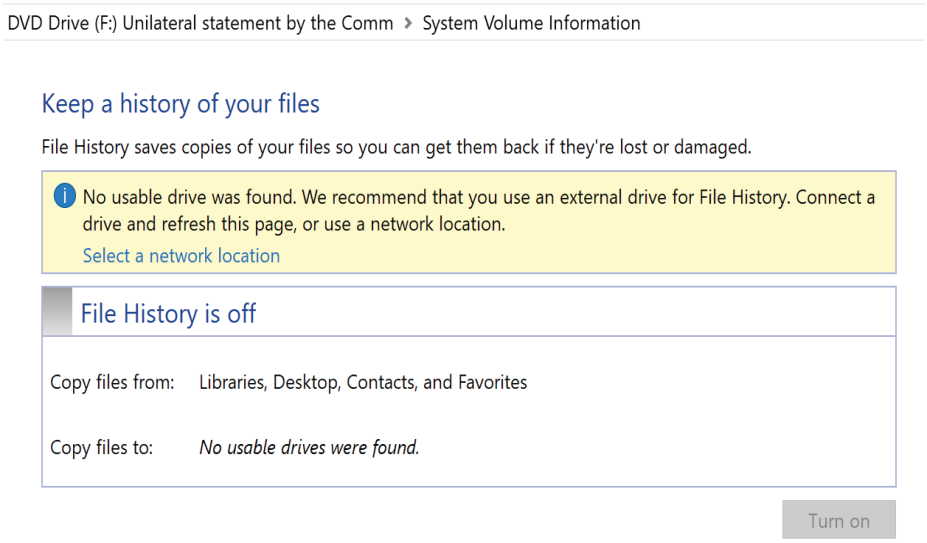


Figure 7: *User is directed to File History navigator upon clicking System Volume Information folder, rather than revealing a series of nested folders containing the PlugX DLL search-order-hijacking triad (Source: Recorded Future)*

The LNK file in this case **(Figure 8)** was simplified compared to the one described in **Figure 5** and no longer used previously reported user metadata, likely in reaction to public reporting highlighting this aspect.

```
"C:\Windows\System32\cmd.exe /q /c "System Volume Information\ \ \ \test.chs"
```

Figure 8: *Simplified LNK argument observed in November 2022 RedDelta activity (Source: Recorded Future)*

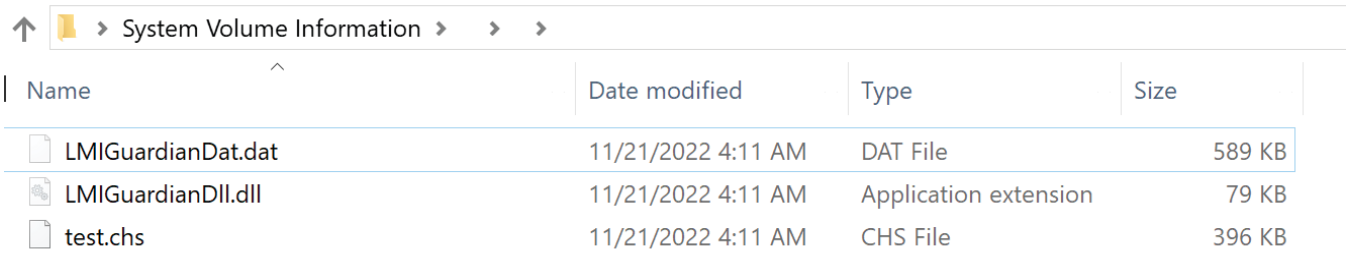


Figure 9: *Nested hidden folders of "System Volume Information" containing PlugX DLL search-order-hijacking triad (Source: Recorded Future)*

Use of European Government Trade- and Migration-Themed Decoy Documents

In all identified RedDelta samples observed from August to November 2022, the user was shown a decoy document specific to government and migration policy within Europe, including: an Austrian immigration program (Red-White-Red Card); a European Union (EU) trade and migration policy; Serbia's EU accession application; and political guidance on the EU's approach toward Russia. These samples ultimately load the group's customized variant of the PlugX backdoor. Notably, in at least one case the group appeared to have edited a publicly available document (the European Commission Serbia Report 2022) to make it appear more sensitive. This included the inclusion of "SENSITIVE" and "need to know" distribution markings with the rest of the document remaining unchanged, despite the finalized version being publicly available at the time of the observed activity. We previously observed RedDelta using a similar tactic to mark a publicly available United Nations General Assembly report as an "Advanced Unedited Version".

In each case, all the necessary components for loading the final payload are included within the initial container file. Earlier in 2022, the group regularly employed an interim stage where a loader fetched all of these components from a remote actor-controlled server. This loader step has been replaced by the aforementioned use of LNK files and, more recently, by the use of archive files with an ISO file.

Shortcut File	Legitimate Binary Used for DLL Search Order Hijacking	Malicious Loader DLL	Encrypted PlugX Payload
Written comments of Hungary.doc.lnk	LMIGuardianSvc.exe (renamed test.msd)	LMIGuardianDll.dll	LMIGuardianDll.dat
SHA256: 720263e2330c07c1def2e63ca722272c1cc3b30ebea6bd7b96d9e4826803cc7	SHA256: 26c855264896db95ed46e502f2d318e5f2ad25b59bdc47bd7ffe92646102ae0d	SHA256: e5e396be385d38f69566aa141de3030ffe4eaad8afb244a2c22df4b6db425478	SHA256: ef2b6b411b79f751d73e824302ca00ff9f0d759a6eea02d2cfb11390d0e9379b
Unilateral statement by the Commission on migration.docx.lnk	LMIGuardianSvc.exe (renamed test.chs)	LMIGuardianDll.dll	LMIGuardianDll.dat
SHA256: c50f7305bd1d085e642588e16fb130bced4a69eae0b0fc48c1c93e4935dc70d4	SHA256: 26c855264896db95ed46e502f2d318e5f2ad25b59bdc47bd7ffe92646102ae0d	SHA256: b35a9716e180b6a4cc92ccdc5d5825c62a41b4f13c0e38b757b2f47b202fc012	SHA256: d6e0903b9d9464c90c2007d84e8cf2387359c693a04c349cf0b551e65f860181
Godišnji izveštaj EK o Srbiji.pdf.lnk	LMIGuardianSvc.exe (renamed svc.tmt)	LMIGuardianDll.dll	LMIGuardianDat.dat
SHA256: 0055e6385633ca35ab3ac70f56d18d90b8d5a5894a5d8e738e567c3f7fb337be	SHA256: 26c855264896db95ed46e502f2d318e5f2ad25b59bdc47bd7ffe92646102ae0d	SHA256: 397cc7543c3b485d9d6ad4d9bc1b25ad098b6484b6a1c4edbd71558103ab0eb3	SHA256: 1765476a354244c6acba50b8f948d2afe23963ecc3a4cbf1f890a7385562d919
General background to the Red-White-Red - Card.doc.lnk	AcroDist.exe (renamed test.tmt)	AcroDistDLL.dll	AcroScan.dat
SHA256: becdb31a669676dac3e797fb6db482f9fd644853e73fc28eb0031bd58487d081	SHA256: 01b68a0c13032bb59f262ed94d2daf85e50fad7a1502a3097029b66b7eb4f903	SHA256: adb61bb5e3941e3824f57e98b2739a00ce4d6e3aa4af2257f99c9698f584753a	SHA256: bfa84b7b4802a480fab498a16a1d177c46495df8f4f950f5d73e9cb220988e2a
Political Guidance for the new EU approach towards Russia.doc.lnk	ClassicExplorerSettings.exe (renamed test.bpu)	ClassicExplorer32.dll	ClassicExplorerLog.dat
SHA256: 3e33897fcbf2f830b665489017a843146955ef67061bd58f004c418b6b97e9ea	SHA256: b44cc792ae7f58e9a12a121c14a067ee1dd380df093339b4bf2b02df5937b2af	SHA256: 8e27900949a087349488d82e7434937bd253d31749041bb0233000a7339fc3e1	SHA256: 9c1ea202237726984b754d17528cfab0212ff9587bbffaf01c8535277b01c24a
State of play in EU trade policy.docx.lnk	AcroDist.exe	AcroDistDLL.dll	AcroScan.dat
SHA256: 131209d5e752300d4af86375abd81d244467b50238e2ffecf62239efaec6e361	SHA256: 01b68a0c13032bb59f262ed94d2daf85e50fad7a1502a3097029b66b7eb4f903	SHA256: 7afbd413c8df77b0c1e0de046c6a726b5afce28efc06f7986c1d8c107cfa89b1	SHA256: 458e19df6dc3402b2b12f473c9aec138d64a289c1539a92dd70cfae281c58838

Table 1: *RedDelta samples observed from August to November 2022, all featuring Europe-themed filename lures and decoy documents. The use of the string "test" was observed frequently within RedDelta filenames, PlugX config campaign IDs, and TLS certificates over this period. (Source: Recorded Future)*

Federal Ministry
Republic of Austria
Interior

July 2022

Information
Red-White-Red - Card

General background to the Red-White-Red - Card:

- "Red-White-Red - Card"was introduced in 2011 and has been successful
- Requirements for "Red-White-Red - Card" (before the amendment takes effect)
  - Concrete job offer
  - no danger to public order and security
  - Sufficient means of subsistence
  - Health insurance (which is a given in the public health insurance system of Austria)
  - Special granting requirements depending on the "pillar"
- "Pillars" of the Red-White-Red Card:
  - **Very highly qualified persons**, e.g. top managers, professors: possibility of a 6-month visa to seek work, no labour market examination, no minimum wage
  - **Skilled workers in shortage occupations**, e.g. lathe operators, milling cutters: annual determination of shortage occupations by the Skilled Workers Regulation of the Federal Ministry of Labour, minimum wage according to collective agreement, no labour market test
  - **Other key workers**: minimum wage (2022: for under 30-year-olds: € 2,835 gross per month, for over 30-year-olds: € 3,402 gross per month), labour market test
  - **University graduates**: at least completion of a Bachelor's degree or Master's degree from the 2nd stage of studies in Austria, minimum wage (2022: € 2,551.50 gross per month), no labour market test
  - **Self-employed key workers**: overall economic benefit for Austria (proof through investment capital of at least € 100,000 in Austria, creation/securing of jobs, transfer of know-how or significant importance in the region), no points system
  - **Start-up founders**: new company to be founded with innovative product, service, process or technology and points system
- Skilled Workers Regulation 2022:
  - On a nationwide list for the year 2022: 66 occupations
  - In addition, there are regional lists in all provinces except Vienna, in which a further 59 shortage occupations are defined for 2022
- Application can be submitted by
  - Applicant/migrant himself and
  - the employer

1

After a slow year, the EU's free trade agenda is picking up speed under the Czech EU Council presidency. Nevertheless, more momentum still seems to be on the unilateral trade measures currently being negotiated in the bloc.

In early 2021, the European Commission presented a new trade strategy, arguing for an "open, sustainable, and assertive trade policy." However, from these three goals, "the openness has been a little bit neglected", a senior EU diplomat told EURACTIV.

One reason for this is structural. In a geopolitically more tense environment where trade dependencies are levered for political purposes, assertiveness seems more urgent than further opening up.

The other reason was timing, with the French government having blocked any major trade deal ahead of the French presidential and parliamentary elections earlier this year.

That is why member state trade ministers focused on toughening up EU trade policy under the French presidency of the EU Council. They made access to public procurement in the EU dependent on mutual access, agreed on a regime to restrict the distorting influence of foreign subsidies, and started to discuss the proposal for an anti-coercion tool.

More sustainability

The EU also moved on to the sustainability pillar of its trade strategy. In June, the Commission presented a proposal to strengthen the role of trade and sustainable development chapters in free trade agreements.

The proposal was welcomed by the European Parliament's trade committee and is not being discussed among member states. "Council Conclusions on the sustainability review are possible in November," a senior EU diplomat said, adding that, so far, discussions had not brought to light many contentious issues.

On the free trade front, meanwhile, some movement was seen in June with the start of negotiations over a free trade agreement with India and with the conclusion of free trade negotiations with New Zealand.

And there is more in the pipeline. A free trade deal with Chile, blocked by France last year, is now ready to be signed, but it is yet unclear whether the new Chilean government will want to get some changes into the deal.

Progress with relatively small trade partners

Non-paper EE, LT, LV, PL
30 September 2022.

Political Guidance for the new EU approach towards Russia

Through the unprovoked and unjustified military aggression against Ukraine, Russia is grossly violating international law and the UN Charter, undermining European security and security of European citizens. The armed aggression against Ukraine is showing Moscow's readiness to use the highest level of military force, regardless of legal or humanitarian considerations, combined with hybrid tactics, cyberattacks and foreign information manipulation and interference, economic and energy coercion, aggressive nuclear rhetoric and nuclear incident threat.

Through armed interference in Georgia and Ukraine, the *de facto* control over Belarus, as well as the continued presence of Russian troops in protracted conflicts, including in the Republic of Moldova, the Russian government is actively aiming to establish so-called spheres of influence. In other theatres such as Libya, Syria, Central African Republic and Mali, Russia also uses ongoing crises in order to undermine EU's interests, including via the means of disinformation and mercenaries.

The threat posed by Russia is the most serious challenge the EU needs to tackle since its inception. The way in which the Union deals with this threat will define the EU's role as a global actor and help handling other serious challenges to EU's security coming from different directions.

In March 2022 **we agreed our Strategic Compass** where we evaluated general global situation in the world and established our respective worldwide long-term strategy. Based upon its findings and taking into account Russia's war crimes, unspeakable atrocities, illegal annexation of Ukrainian territory, its irresponsible nuclear blackmail as well as escalatory mobilization decisions **we need to communicate our new - more focused EU approach to Russia**.

It is crucial to ensure the Member States' involvement in defining the scope of such framework. We suggest to formulate it in a concise, targeted way of short **political guidance** which may read as follows:

Russia, under its present leadership, remains consistently an aggressive state working on a doctrine of state imperialism, openly declaring an intention to further violate principles of international order if its suits its interest, including through annexation of further territories. That is why the threat **Russia poses goes far beyond Ukraine. Russia constitutes to be a direct multifaceted threat to Europe and the whole world community**.

Therefore the EU should not only be ready to effectively counter RU malign actions, but develop tools for more proactive **long term deterrence and containment**.

EU actions should include:

1. **Ensuring, together with international partners like the US, the NATO allies and a broad international coalition, that Russia is brought to a strategic defeat** in its aggression against Ukraine. This must be done especially by:

1.1 supporting Ukraine militarily, financially and politically until it regains its territory within the internationally recognized borders (in particular delivery of heavy weapons and training is of utmost importance) as well as after the war in order to assist in its reconstruction and stability;

1.2 safeguarding the international law through maintenance and enhancement of sanctions and isolation policy until Russia withdraws from the territory of Ukraine, brings those responsible for war crimes and the crime of aggression to justice and pays for reconstruction;

1.3 creating conditions that will prevent any future use of Russian military forces against Ukraine and ensure long term stability in the region;

Unilateral statement by the Commission on migration (n. 8)
"Joint text on the general budget of the European Union for the financial year 2022"
(Annex n. 2)

"*Given the continuing needs foreseen in the coming years, the Commission confirms its plan to ensure that the average annual funding for migration for the Southern Neighborhood from the NDICI-GE Neighborhood allocation and, if needed, from other instruments, remains at least at the level envisaged for 2022*".

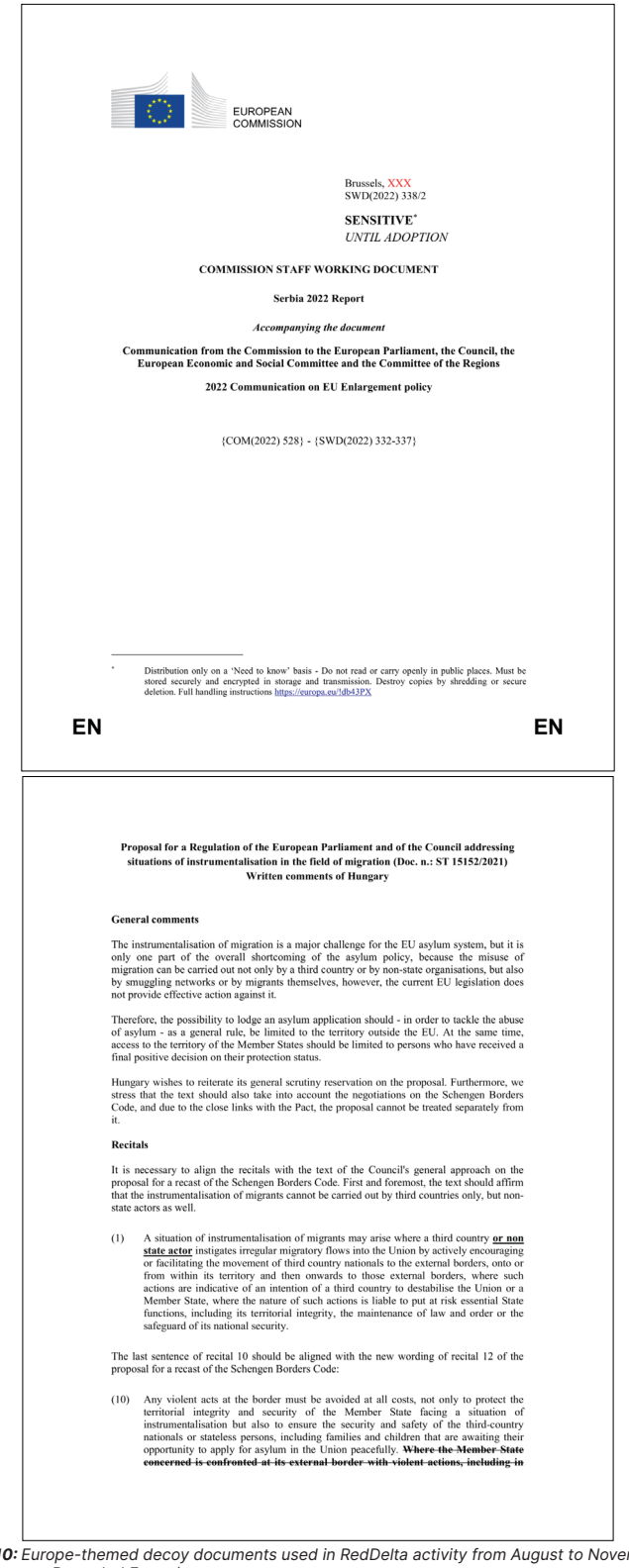
We "MED5" Countries - i.e. CY, EL, ES, IT and MT - reiterate our strong concern about the inadequate of 2023 financial allocations for migration to the Southern Neighborhood, through NDICI-GE Neighborhood. The amount of proposed appropriations does not correspond to the Commission's assurance in the declaration annexed to the 2022 Budget, cited above.

In the context of the conciliation procedure for the EU budget 2023, we MED5 call on the Commission to keep a high profile on all current migration crises, but to respect its commitment to migration for the Southern Neighborhood, by ensuring for 2023 at least the level of funding foreseen for 2022.

We therefore ask the Commission to provide - before the ECOFIN budget of 11 November - up-to-date estimates of resources for the Southern Neighborhood to meet its commitment, with the breakdown of sources both by NDICI-GE Neighborhood and by "other instruments" (as repeatedly mentioned by the Commission itself).

For the above, we MED5 inform the Presidency that, if necessary, we are available, under the current 2023 budget procedure, to open negotiations towards possible reinforcements of the NDICI-GE, on the basis of targeted amendments by European Parliament.

We also ask the Presidency that, if the Declaration no 2 - attached to the Council position of 6 September 2022 - needs to be updated to reflect the current situation, the amendments in no way invalidate the part stating that "the current uncertainties and consequences of the war in Ukraine affect food security in the southern neighborhood".



EUROPEAN COMMISSION

Brussels, XXX
SWD(2022) 338/2

SENSITIVE*
UNTIL ADOPTION

COMMISSION STAFF WORKING DOCUMENT

Serbia 2022 Report

Accompanying the document

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions

2022 Communication on EU Enlargement policy

{COM(2022) 528} - {SWD(2022) 332-337}

* Distribution only on a 'Need to know' basis - Do not read or carry openly in public places. Must be stored securely and encrypted in storage and transmission. Destroy copies by shredding or secure deletion. Full handling instructions https://europa.eu/!dh43PX

EN **EN**

Proposal for a Regulation of the European Parliament and of the Council addressing situations of instrumentalisation in the field of migration (Doc. n.: ST 15152/2021)
Written comments of Hungary

General comments

The instrumentalisation of migration is a major challenge for the EU asylum system, but it is only one part of the overall shortcoming of the asylum policy, because the misuse of migration can be carried out not only by a third country or by non-state organisations, but also by smuggling networks or by migrants themselves, however, the current EU legislation does not provide effective action against it.

Therefore, the possibility to lodge an asylum application should - in order to tackle the abuse of asylum - as a general rule, be limited to the territory outside the EU. At the same time, access to the territory of the Member States should be limited to persons who have received a final positive decision on their protection status.

Hungary wishes to reiterate its general scrutiny reservation on the proposal. Furthermore, we stress that the text should also take into account the negotiations on the Schengen Borders Code, and due to the close links with the Pact, the proposal cannot be treated separately from it.

Recitals

It is necessary to align the recitals with the text of the Council's general approach on the proposal for a recast of the Schengen Borders Code. First and foremost, the text should affirm that the instrumentalisation of migrants cannot be carried out by third countries only, but non-state actors as well.

(1) A situation of instrumentalisation of migrants may arise where a third country **or non state actor** instigates irregular migratory flows into the Union by actively encouraging or facilitating the movement of third country nationals to the external borders, onto or from within its territory and then onwards to those external borders, where such actions are indicative of an intention of a third country to destabilise the Union or a Member State, where the nature of such actions is liable to put at risk essential State functions, including its territorial integrity, the maintenance of law and order or the safeguard of its national security.

The last sentence of recital 10 should be aligned with the new wording of recital 12 of the proposal for a recast of the Schengen Borders Code:

(10) Any violent acts at the border must be avoided at all costs, not only to protect the territorial integrity and security of the Member State facing a situation of instrumentalisation but also to ensure the security and safety of the third-country nationals or stateless persons, including families and children that are awaiting their opportunity to apply for asylum in the Union peacefully. ~~**Where the Member State concerned is confronted at its external border with violent actions, including in**~~

Figure 10: *Europe-themed decoy documents used in RedDelta activity from August to November 2022 (Source: Recorded Future)*

PlugX Loading Mechanism and Payload

After being executed through the legitimate binary, the DLL loader is responsible for decrypting the PlugX payload (the .dat files listed in **Table 1**) prior to passing execution off to them. While RedDelta has consistently updated the decryption routine used, we have observed this routine changing more frequently throughout 2022. The developers of the PlugX variant used in RedDelta activity had previously used a prepended XOR key, but have since switched to various iterations of XOR decryption schemes that don't rely on the XOR key being prepended to the file.

Sample File Name(s)	PlugX Payload Decoding Technique	Config Decryption Key
State of play in EU trade policy.zip (August 2022)	The formula for this sample is `((~key & 0x55 | 0x00 | key & 0xAA)& 0xff) ^ (~byte & 0x55 | byte & 0xAA)`. However, this can be simplified down to byte ^ key. For either formula, the key is incremented by the same hardcoded value between each XOR operation. The decryption begins a few bytes from the start of the file.	ax5Mg76v9
General background to the Red-White-Red - Card.zip (October 2022) Political Guidance for the new EU approach towards Russia.rar (October 2022)	The formula for these samples is byte ^ `((key - (0x00 - filesize)) & 0xff)`. In these samples, the "key" value in the formula above changes each iteration of the loop. The value in the subsequent iteration is the final XOR value calculated in the one before. The first iteration uses a hard-coded "seed" value for the "key" value.	ax5Mg76v9

Sample File Name(s)	PlugX Payload Decoding Technique	Config Decryption Key
Unilateral statement by the Commission on migration.iso (November 2022) SWC 202022.iso (November 2022) Written comments of Hungary.rar (December 2022)	The formula for these is byte ^ `((key + (filesize>>1)) & 0xff)`. In these samples, the "key" value in the formula above changes each iteration of the loop. The value in the subsequent iteration is the final XOR value calculated in the one before. The first iteration uses a hard-coded "seed" value for the "key" value.	jOh752oCI

Table 2: *Evolution in payload-encoding mechanism observed in RedDelta PlugX samples from August to November 2022 (Source: Recorded Future)*

The PlugX samples continue to use an encrypted configuration that contains values such as C2, mutex, file path, decoy document file name, and a custom marker (extracted configurations are included in **Appendix C**). The mutex and file path continue to follow a pattern of being named after the legitimate executable filename followed by 3 (file path) or 6 (mutex) random letters. This has been a consistent attribute of RedDelta PlugX use for several years.

All of the PlugX files contain a decoy document in the overlay section of the Windows executable that is subsequently shown to the user, as displayed in **Figure 10**. The HTTP POST headers observed in the latest PlugX samples also remain identical to versions described in ESET and Proofpoint reporting from March 2022, with the exception of the hard-coded User-Agent value.

? **POST** https://62.233.57.49/ LMIGuardian...

Remote address:
62.233.57.49:443

Request
```
POST / HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 10.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR
3.0.30729; .NET CLR 3.5.30729)
Sec-Dest: 6BaFwgxQ
Sec-Site: 846FF6D55FBC89EEE96E
Content-Length: 1100
Host: 62.233.57.49
```

Response
```
HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 0
```

Figure 11: *Request headers and server response observed in RedDelta's customized PlugX variant (Source: Recorded Future Triage)*

Mitigations

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking illicit connection attempts from — the external IP addresses and domains listed in **Appendix A**.
- Where possible, alert on use of known disk image file types, such as ISO, and shortcut files, which have been increasingly abused by threat actors in recent times. Furthermore, organizations should consider disabling auto-mounting of ISO files.
- Practice network segmentation and ensure special protections exist for sensitive information, such as multi-factor authentication and extremely restricted access and storage on systems only accessible via an internal network.
- Disable basic and legacy authentication where possible, as these can allow attackers to bypass in-place security measures.
- Keep all software and applications up to date — in particular, operating systems, antivirus software, and core system utilities.
- Filter email correspondence and scrutinize attachments for malware.
- Employ host-based controls; one of the best defenses and warning signals to thwart attacks is to conduct client-based host-logging and intrusion detection capabilities.
- Implement basic incident response and detection deployments and controls like network IDS, netflow collection, host-logging, and web proxy, alongside human monitoring of detection sources.

Outlook

RedDelta continues to be a highly persistent threat activity group conducting operations targeting organizations across Asia and Europe. Throughout 2022, we have identified RedDelta operators iterating and adding new defense evasion and anti-analysis methods to the group's customized PlugX variant at a rapid pace. Despite this, many elements of the group's TTPs have remained consistent over time. While RedDelta has shown a propensity for targeting certain geographic regions over many years, particularly Vietnam and Myanmar, the group has also demonstrated the ability to quickly shift targeting in line with emerging geopolitical developments.

Appendix A — Indicators of Compromise

Network Infrastructure:

Below is a list of IP addresses used by RedDelta active in November/December 2022 (as of 2022/12/06):

5.34.182[.]68	(last seen:2022/12/06)
38.55.105[.]46	(last seen:2022/12/06)
43.154.25[.]220	(last seen:2022/12/06)
45.90.59[.]153	(last seen:2022/12/06)
45.147.26[.]45	(last seen:2022/12/06)
82.118.21[.]86	(last seen:2022/12/06)
88.218.193[.]76	(last seen:2022/12/06)
88.218.193[.]247	(last seen:2022/12/06)
103.192.226[.]46	(last seen:2022/12/06)
103.192.226[.]87	(last seen:2022/12/06)
114.115.138[.]44	(last seen:2022/12/06)
185.80.201[.]4	(last seen:2022/12/06)
62.233.57[.]49	(last seen:2022/12/01)
185.14.29[.]26	(last seen:2022/11/15)

Additional select historical IP addresses used by RedDelta from March to October 2022 (please note that VPS IP addresses are ephemeral indicators and change ownership over time):

195[.]123[.]208[.]140	(last seen:2022/10/31)
45.32.101[.]7	(last seen:2022/10/30)
5.34.178[.]156	(last seen:2022/10/30)
5.34.176[.]17	(last seen:2022/10/13)
107.181.160[.]16	(last seen:2022/10/06)
103.79.120[.]71	(last seen:2022/10/02)
103.79.120[.]68	(last seen:2022/09/23)
103.79.120[.]70	(last seen:2022/09/11)
184.164.89[.]173	(last seen:2022/09/10)
82.118.21[.]248	(last seen:2022/08/27)
103.79.120[.]72	(last seen:2022/08/18)
64.34.216[.]44	(last seen:2022/08/17)
64.34.205[.]178	(last seen:2022/08/16)

64.34.216[.]50 (last seen:2022/08/15)

64.34.205[.]41 (last seen:2022/06/28)

64.34.205[.]45 (last seen:2022/06/28)

107.178.71[.]200 (last seen:2022/06/27)

107.167.64[.]6 (last seen:2022/06/25)

69.90.190[.]110 (last seen:2022/06/15)

185.239.226[.]7 (last seen:2022/06/15)

45.134.83[.]29 (last seen:2022/06/12)

104.255.174[.]59 (last seen:2022/05/24)

104.255.174[.]60 (last seen:2022/05/24)

104.255.174[.]58 (last seen:2022/05/20)

43.254.218[.]128 (last seen:2022/05/15)

104.255.174[.]54 (last seen:2022/05/03)

104.255.174[.]55 (last seen:2022/05/03)

104.255.174[.]53 (last seen:2022/05/02)

155.94.200[.]214 (last seen:2022/04/27)

155.94.200[.]215 (last seen:2022/04/27)

155.94.200[.]216 (last seen:2022/04/27)

69.90.184[.]125 (last seen:2022/04/22)

155.94.200[.]211 (last seen:2022/04/13)

155.94.200[.]206 (last seen:2022/04/12)

155.94.200[.]209 (last seen:2022/04/12)

103.192.226[.]38 (last seen:2022/03/24)

103.107.104[.]6 (last seen:2022/03/18)

107.167.64[.]4 (last seen:2022/03/09)

Domains:

microsite-manager[.]com

mashupdatabase[.]com

blogdirve[.]com

Malware Samples:

1aeb51a19fb0162d8c0cf5bc27f666a2885d4497b1738f6ad9c7125a8bc3c2d9
Unilateral statement by the Commission on migration.iso

c50f7305bd1d085e642588e16fb130bced4a69eae0b0fc48c1c93e4935dc70d4
Unilateral statement by the Commission on migration.docx.lnk

b35a9716e180b6a4cc92ccdc5d5825c62a41b4f13c0e38b757b2f47b202fc012
LMIGuardianDll.dll

d6e0903b9d9464c90c2007d84e8cf2387359c693a04c349cf0b551e65f860181
LMIGuardianDll.dat

84cc77c788e3f5848893fb8b3cf3085d951d942ed79cae357984e42a27024e6e
Written comments of Hungary.rar

720263e2330c07c1def2e63ca722272c1cc3b30ebea6bd7b9c6d9e4826803cc7
Written comments of Hungary.doc.lnk

e5e396be385d38f69566aa141de3030ffe4eaad8afb244a2c22df4b6db425478
LMIGuardianDll.dll

ef2b6b411b79f751d73e824302ca00ff9f0d759a6eea02d2cfb11390d0e9379b
LMIGuardianDll.dat

5b027ada26a610e97ab4ef9efb1118b377061712acec6db994d6aa1c78a332a8
SWC 202022.iso

0055E6385633CA35AB3AC70F56D18D90B8D5A5894A5D8E738E567C3F7FB337BE
Godišnji izveštaj EK o Srbiji.pdf.lnk

397cc7543c3b485d9d6ad4d9bc1b25ad098b6484b6a1c4edbd71558103ab0eb3
LMIGuardianDll.dll

1765476a354244c6acba50b8f948d2afe23963ecc3a4cbf1f890a7385562d919
LMIGuardianDat.dat

f70d3601fb456a18ed7e7ed599d10783447016da78234f5dca61b8bd3a084a15
Political Guidance for the new EU approach towards Russia.rar

8e27900949a087349488d82e7434937bd253d31749041bb0233000a7339fc3e1
ClassicExplorer32.dll

3e33897fcbf2f830b665489017a843146955ef67061bd58f004c418b6b97e9ea
Political Guidance for the new EU approach towards Russia.doc.lnk

9c1ea202237726984b754d17528cfab0212ff9587bbffaf01c8535277b01c24a
ClassicExplorerLog.dat

7558ff23586298a27fd504558884c880bcd17cd9ccf5379587c61be03653fd7a
State of play in EU trade policy.zip

7afbd413c8df77b0c1e0de046c6a726b5afce28efc06f7986c1d8c107cfa89b1
AcroDistDLL.dll

131209d5e752300d4af86375abd81d244467b50238e2ffecf62239efaec6e361
State of play in EU trade policy.docx.lnk

458e19df6dc3402b2b12f473c9aec138d64a289c1539a92dd70cfae281c58838
AcroScan.dat

79f5c7ee5f1cd22759816c0b90dc9ac8427c9e5450be8b0395cb49dd0ff4e284
General background to the Red-White-Red - Card.zip

becdb31a669676dac3e797fb6db482f9fd644853e73fc28eb0031bd58487d081
General background to the Red-White-Red - Card.doc.lnk

adb61bb5e3941e3824f57e98b2739a00ce4d6e3aa4af2257f99c9698f584753a
AcroDistDLL.dll

bfa84b7b4802a480fab498a16a1d177c46495df8f4f950f5d73e9cb220988e2a
AcroScan.dat

Appendix B — Mitre ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure — Virtual Private Server	T1583.003
Resource Development: Acquire Infrastructure — Domains	T1583.001
Initial Access: Phishing Spearphishing Attachment	T1566.001
Initial Access: Phishing — Spearphishing Link	T1566.002
Execution: User Execution — Malicious File	T1204
Defense Evasion: Hijack Execution Flow — DLL Search Order Hijacking	T1574.001
Defense Evasion: Deobfuscate/Decode Files or Information	T1140
Defense Evasion: Hide Artifacts — Hidden Files and Directories	T1564.001
Defense Evasion: Hide Artifacts — Hidden Window	T1564.003
Defense Evasion: Masquerading — Match Legitimate Name or Location	T1036.005
Defense Evasion: Masquerading — Double File Extension	T1036.007
Command-and-Control: Encrypted Channel: Symmetric Cryptography	T1573.001
Command-and-Control: Data Encoding: Standard Encoding	T1132.001
Exfiltration: Exfiltration over C2 Channel	T1041

Appendix C — Extracted PlugX Configs

Config Field	Value
Decoy Document Name	General background to the Red-White-Red-Card.docx
Mutex	AcroDistMGzXRY
File Path	AcroDistJBM
Marker	test2023
C2 - 1	107.181.160[.]16:443
C2 - 2	107.181.160[.]16:443
C2 - 3	107.181.160[.]16:443

Table 3: Extracted config from bfa84b7b4802a480fab498a16a1d177c46495df8f4f950f5d73e9cb220988e2a (Source: Recorded Future)

Config Field	Value
Decoy Document Name	State of play in EU trade policy.docx
Mutex	AcroDistBGoFSQ
File Path	AcroDistDlr
Marker	eu
C2 - 1	64.34.205[.]178:443
C2 - 2	64.34.205[.]178:443
C2 - 3	64.34.205[.]178:443

Table 4: Extracted config from 458e19df6dc3402b2b12f473c9aec138d64a289c1539a92dd70cfae281c58838 (Source: Recorded Future)

Config Field	Value
Decoy Document Name	Political Guidance for the new EU approach towards Russia.docx
Mutex	ClassicExplorepDvoov
File Path	ClassicExploreFvN
Marker	test222
C2 - 1	5.34.178[.]156:443
C2 - 2	5.34.178[.]156:443
C2 - 3	5.34.178[.]156:443

Table 5: Extracted config from 9c1ea202237726984b754d17528cfab0212ff9587bbffaf01c8535277b01c24a (Source: Recorded Future)

Config Field	Value
Decoy Document Name	Unilateral statement by the Commission on migration.docx
Mutex	LMIGuardianEsKRrY
File Path	LMIGuardianjlg
Marker	test
C2 - 1	62.233.57[.]49:443
C2 - 2	62.233.57[.]49:443
C2 - 3	62.233.57[.]49:443

Table 6: Extracted config from 1aeb51a19fb0162d8c0cf5bc27f666a2885d4497b1738f6ad9c7125a8bc3c2d9 (Source: Recorded Future)

Config Field	Value
Decoy Document Name	Godišnji izveštaj EK o Srbiji.pdf
Mutex	LMIGuardianRqEbeL
File Path	LMIGuardianqqH
Marker	ser
C2 - 1	62.233.57[.]49:443
C2 - 2	62.233.57[.]49:443
C2 - 3	62.233.57[.]49:443

Table 7: Extracted config from 5b027ada26a610e97ab4ef9efb1118b377061712acec6db994d6aa1c78a332a8 (Source: Recorded Future)

Config Field	Value
Decoy Document Name	Written comments of Hungary.docx
Mutex	LMIGuardianvSqtmC
File Path	LMIGuardianpfc
Marker	test
C2 - 1	45.90.59[.]153:443
C2 - 2	45.90.59[.]153:443
C2 - 3	45.90.59[.]153:443

Table 8: Extracted config from 84cc77c788e3f5848893fb8b3cf3085d951d942ed79cae357984e42a27024e6e (Source: Recorded Future)

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,500 businesses and government organizations across 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.