

# DarkCasino行动：APT组织Evilnum近期攻击事件深入分析

[blog.nsfocus.net/darkcasino-apt-evilnum/](http://blog.nsfocus.net/darkcasino-apt-evilnum/)

伏影实验室

## 一、概述

近期，绿盟科技伏影实验室捕获了一系列针对欧洲国家的网络钓鱼活动。这些活动主要针对线上赌博平台，目标为通过攻击此类服务背后的活跃的线上交易行为，窃取服务商和消费者的交易凭据，进而获取非法收益。

通过深入分析，伏影实验室确定该系列活动是APT组织Evilnum近期攻击活动 (<http://blog.nsfocus.net/agentvxapt-evilnum/>) 的延续。与既往活动相比，Evilnum攻击者在本次行动中继承了其代表性的攻击手法，但使用了更多样的攻击流程与复杂的攻击组件，并启用了两种新型木马程序DarkMe与PikoloRAT，展现了其较高的工具开发能力、流程设计能力与丰富的攻防对抗经验。同时，因为不同攻击流程的设计思路与具体实现存在明显差异，伏影实验室认为有多个攻击者同时参与了此次行动。

通过提取攻击目标与主要木马程序的关键词并组合，伏影实验室将Evilnum的该起行动命名为DarkCasino。该起行动表明Evilnum仍然以在线交易平台为主要目标，能够迅速发现网络犯罪机会并执行攻击。

截至报告发布时，该DarkCasino行动仍在持续。

## 二、组织信息

Evilnum是一个在2018年被发现的APT组织，活跃于英国和欧盟国家，主要攻击目标为金融科技公司，目的为通过窃取交易凭证盗取公司或个人账户资金。组织名称Evilnum来自同名的木马程序，亦被卡斯基称为DeathStalker。

Evilnum的代表性攻击手段是将恶意程序伪装成客户的身份证明文件，欺骗金融公司的工作人员运行这些程序，进而通过植入间谍木马获得受害者主机上的高价值信息。

Evilnum有较强的开发能力，能够设计复杂的攻击流程和攻击组件。绿盟科技伏影实验室曾捕获和披露该组织具有高完成度的攻击流程和一款stub型木马AgentVX。

## 三、影响面分析

分析发现，Evilnum本次行动的受害者主要分布于地中海区域的欧洲国家以及加拿大、新加坡、菲律宾等相关国家，其直接攻击目标包括线上赌场平台、使用此类平台的各国消费者以及与平台线上交易行为有关的其他人员。

已发现的攻击流程中，Evilnum使用以下字符串作为诱饵文件名：

### 诱饵文件名

offer deal visa 2022.lnk

offer crypto casino.scr

Scatters Casino offers Daily Promotions.pif

new casino crypto.com

Promo CPL CPA Traffic.com

PayRedeemUpdateIntegration19052022.scr

DOCUMENTATION AGREEMENTS S CONSULTING INTEGRATION.pif

上述内容中的Scatters Casino是一家由马耳他公司Gammix Limited运营的线上赌场，这些诱饵文件一边尝试将自身伪装为线上交易证明或广告投放服务促销文件以攻击scatters的运营人员，一方面也尝试伪装为scatters促销广告来攻击scatters的用户，从而使Evilnum攻击者能够获取这些目标的主机上保存的交易凭证或相关信息。

对各式诱饵文档的来源进行统计，伏影实验室发现本次DarkCasino活动的受害者广泛分布于马耳他、波兰、塞浦路斯、亚美尼亚、西班牙、瑞士、法国、爱尔兰等欧洲国家，以及加拿大、以色列甚至新加坡、菲律宾等非欧洲国家：



图3.1 DarkCasino行动受害者分布情况

可以发现受害者地理位置以马耳他为核心，辐射至多个可能使用scatters网站服务的国家。

scatters的线上赌场平台成立于2019年，扩张十分迅速。目前，scatters网站声称其线上赌场服务拥有价值2.3亿欧元的奖池，这可能是Evilnum本次行动将其作为目标的主要原因。

此外，一些信息表明，DarkCasino行动有可能是一场规模更大且更持久的网络攻击活动的一部分。IoC关联线索显示，Evilnum的部分资产可以关联至一场从2021年下半年开始延续至2022年年初的，针对加密货币相关交易平台和用户的网络攻击活动。在这场活动中，攻击者主要投递了大量带有签名的ParallaxRAT和NetWire木马，用于窃取目标主机信息，其主要影响目标主要集中在欧洲国家。虽然攻击者在该活动中使用的诱饵形式及网络资源与DarkCasino行动存在一定程度的关联，但伏影实验室尚未获取直接证据证明该活动同样是Evilnum所为，该攻击者可能是以合作的形式借用Evilnum资产并加入其行动中。

## 四、攻击流程分析

本次行动中，Evilnum组织攻击者主要创建了三类不同的攻击流程。三类流程以不同类型的诱饵文件为起始，通过访问公有资源或失陷站点获取隐写图片，提取其中的DarkMe木马载荷内容后用不同的方式加载执行。

### 4.1 攻击流程A

这是Evilnum攻击者最早实现的一类攻击流程，同时也是组件复杂度最高的流程。关键组件的最早发现日期为5月2日。

研究不同的组件时发现，该攻击流程包含两种变型，分别为创建时间为4月28日的，从网络位置获取内容的流程A1；以及创建时间为5月1日的，不需要联网下载内容的流程A2。两种变型的实际执行过程相似。



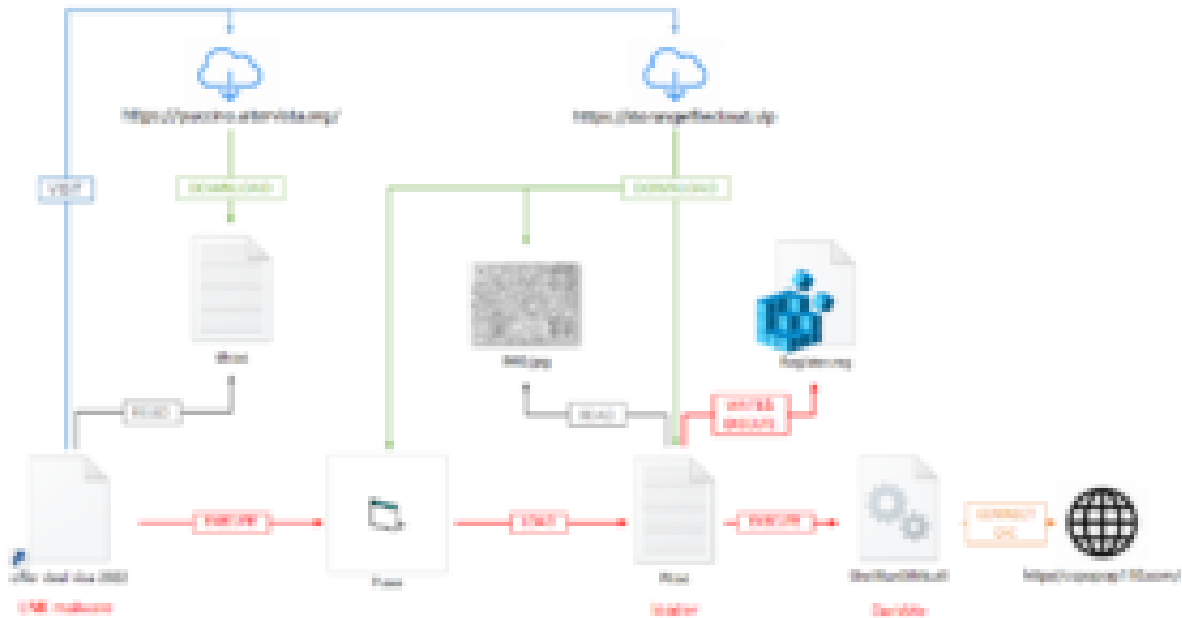


图4.2 DarkCasino攻击流程B

上图为流程B的图示。该过程中，攻击者沿袭了组织的一贯思路，通过投递带有恶意mshta指令的快捷方式诱饵文件，访问受控wordpress站点获取后续的指令代码并运行。

本流程的关键阶段在于通过访问第二阶段站点获取的三个文件P.exe, PI.txt与IMG.jpg。被P.exe加载后，主要loader木马PI.txt会提取IMG.jpg中隐藏的可执行文件ShellRunDllVb.dll，并通过创建名为Register.reg的注册表文件将该dll文件注册为系统组件{A762B0C7-5244-4B3E-ADED-D549E9CEA39E}。loader木马最终通过rundll32 /sta命令执行该组件。

上述操作最终执行的是名为DarkMe的间谍木马程序，通信CnC为cspapop110.com。

### 4.3 攻击流程C

Evilnum攻击者在5月19日补充了一种更精简的流程。

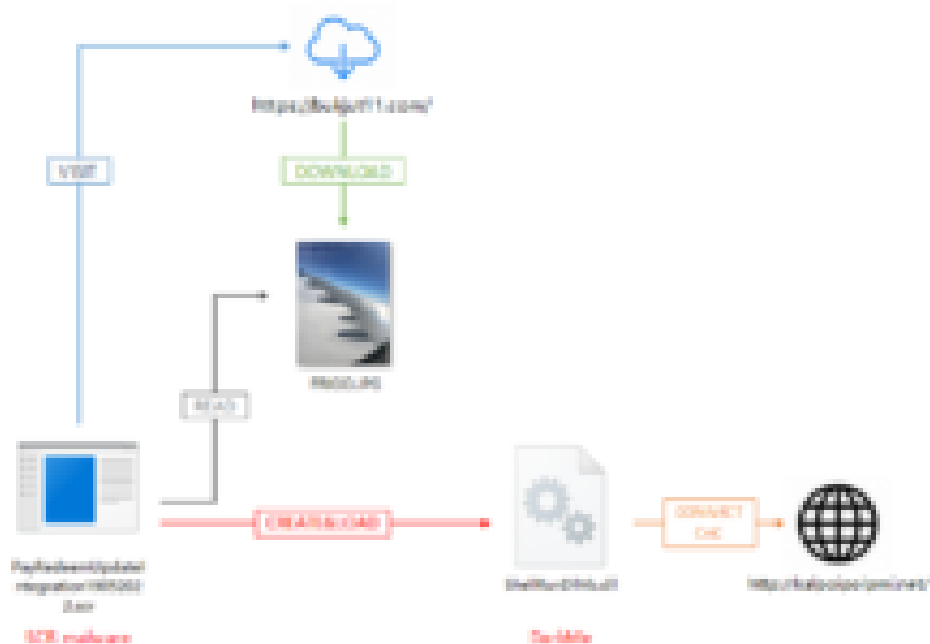


图4.3 DarkCasino攻击流程C

上图为流程C的图示。该流程通过伪装成scr文件的loader木马发起。木马通过直接访问内置的url链接获取一张隐写图像，随后提取其中的ShellRunDllVb.dll文件并加载执行。该dll文件同样是DarkMe木马，通信CnC为kalpoipolpmi.net。

## 五、组件分析

本次行动中，Evilnum主要使用了一种自制的新型木马程序。伏影实验室通过木马程序中的特殊字符串将其命名为DarkMe。

此外，伏影实验室在进行关联分析时发现了另一种与Evilnum本次行动有紧密联系的新型木马程序，并通过其中特殊字符串将其命名为PikoloRAT。

### 5.1 DarkMe

DarkMe是一种VisualBasic间谍木马，由Evilnum攻击者开发并运用在各类攻击流程中。DarkMe的初始版本出现在2021年9月25日，至今已迭代出5个版本。

DarkMe的通信能力通过一种公开的WinSock32模块 (<http://leandroascierto.com/blog/winsoc32/>) 实现。该模块通过创建名为SOCKET\_WINDOW的窗口，以窗口信息的方式与服务端进行套接字通信。

DarkMe木马在该模块的基础上陆续添加了大量功能代码，使其从下载者木马逐渐演变成具有间谍软件能力的stub类型木马。

#### 5.1.1 功能

由于不同版本DarkMe的功能代码不同，此处以本次行动中出现的V5版本木马程序（ShellRunDllVb.dll）进行说明。

该木马在运行后首先会采集宿主机信息并发送至CnC。V4版本收集的信息包括宿主机所在位置缩写、所在国家全称、计算机名、用户名、反病毒软件列表、木马标记以及前台窗口标题，这些信息使用固定分隔符0x3F分隔，并在前部添加固定字符串“92”，形成上线信息并发送至CnC端。

```

00000000 39 32 3f 3f 3f 43 4e 3f 50 65 6f 70 6c 65 27 73 92??N? People's
00000010 20 52 65 70 75 62 6c 69 63 20 6f 66 20 43 68 69  Republi c of Chi
00000020 6e 61 3f                                     na?
00000030                                     3f 4e 6f 20 41 6e 74 69 76  ? No Antiv
00000040 69 72 75 73 3f 70 61 73 73 77 6f 72 64 3f d5 fd  irus?pas sword?..
00000050 d4 da b2 b6 bb f1 20 b1 be b5 d8 c1 ac bd d3 3f  .... . ....?

```

图5.1 DarkMe上线流量

DarkMe实现了多个模块，以支持各类间谍功能。其中一个主要模块名为clsfile，用于实现在CnC控制下的文件操作。CnC控制指令由通信内容的前6字节给出，各指令对应操作如下表：

指令	功能
300100	获取磁盘分卷信息
STRFLS	遍历指定目录获取目录结构
STRFL2	遍历指定目录获取目录结构，支持大型目录
SHLEXE	执行cmd命令
RNMFIL	重命名指定文件
DELDEL	删除指定文件
DIRMAP	创建指定目录
DELMAP	删除指定目录
SEITUS	写入指定文件
SEITUD	读取指定文件
ZIPALO	写入压缩文件
FRIKAT	写入注册表启动项
COPALO	复制指定文件
PASALO	粘贴指定文件

表5.1 DarkMe指令对照表

此外，DarkMe还融合了一套公开代码 (<https://forums.codeguru.com/showthread.php?15579-Save-Screen-Capture-output-to-a-file>)，实现了屏幕截图功能。







8	鼠标移动到指定位置
9	获取剪贴板内容
17	设置屏幕截图间隔
18	设置屏幕截图质量
19	设置屏幕截图缩放尺寸
24	结束自身进程
55	设置临时文件路径
4875	执行cmd命令
4876	执行powershell命令
8888	加载运行PEGASUS HVNC
8889	卸载木马本体
8890	持久化，包括添加自启动项和计划任务
8891	删除持久化内容

表5.2 PikoloRAT指令对照表

可以看到除基本的远控功能外，PikoloRAT还可以通过释放内置的PEGASUS HVNC模块（一种近期泄露的hVNC工具）执行更完善的远程控制。

## 六、技战术分析

### 6.1 覆写式侧加载

本次攻击流程A中，Evilnum攻击者投递了一个恶意的python39.dll文件，并通过合法文件python.exe侧加载该恶意文件。

与常见侧加载构建逻辑不同的是，该恶意python39.dll实际上是通过直接覆写原始python39.dll文件得到的。Evilnum攻击者将一段shellcode直接写入原始python39.dll的函数PyImport\_AddModuleObject的位置，使python39.dll在被加载时自动启动该shellcode。

该设计的好处在于：

操作简便，无需编译独立的dll程序并实现其导出方法；

适用性广，理论上可以对任意合法dll文件进行类似的覆写操作，构建侧加载shellcode攻击链；

隐蔽性强，覆写后dll文件与原始dll文件相似度很高，不易被定位。



```

seg000:000025A5      jz     start_loc_125B2 ; if is064enn
seg000:000025A7      push  5
seg000:000025A9      pop   edi
seg000:000025AB      push  edi
seg000:000025AD      lea   eax, [ebp+ehandle]
seg000:000025AF      push  eax
seg000:000025B1      push  [ebp+var_28]
seg000:000025B3      call  near ptr 0040111F00
seg000:000025B5      add   esp, 80h
seg000:000025B7      jmp   start_loc_125B2
-----|-----
seg000:000025B9      loc_125B2: ; CODE XREF: sub_12409+09C ↑
seg000:000025BB      lea   eax, [ebp+var_160] ; else
seg000:000025BD      push  eax
seg000:000025BF      push  ecx
seg000:000025C1      push  edi
seg000:000025C3      push  ebx
seg000:000025C5      push  [ebp+ehandle]
seg000:000025C7      call  [ebp+HWWriteVirtualMemory]
seg000:000025C9      push  5
seg000:000025CB      pop   edi

```

图6.3 Shellcode注入代码中的X64call调用逻辑

```

seg000:00001EAE      push  ebx
seg000:00001EAF      push  esi
seg000:00001EB0      push  edi
seg000:00001EB1      mov   [ebp+var_4], esp
seg000:00001EB4      and   esp, 0FFFFFFF0h
seg000:00001EB7      push  33h ; '3'
seg000:00001EB9      call  $+5
seg000:00001EBE      add   [esp+58h+var_58], 5
seg000:00001EC2      retf

```

图6.4 X64call调用代码

这种技巧同样可以起到规避api检测的效果。

### 6.3 图片隐写

本次行动中，Evilnum攻击者使用了两种形式的隐写图片。

流程B中，名为IMG.jpg的图片使用了冗余隐写，将恶意代码存放于文件尾部，使用固定字符串(\$HEH\$E)作为分隔标志：

53:4250h:	A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5	FFFFFFFFFFFFFFFF
53:4260h:	A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5	FFFFFFFFFFFFFFFF
53:4270h:	A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5	FFFFFFFFFFFFFFFF
53:4280h:	A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5	FFFFFFFFFFFFFFFF
53:4290h:	A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5	FFFFFFFFFFFFFFFF
53:42A0h:	A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5	FFFFFFFFFFFFFFFF
53:42B0h:	A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5	FFFFFFFFFFFFFFFF
53:42C0h:	A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5	FF 00 ... (\$HEH\$E)
53:42D0h:	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	ME.....??.
53:42E0h:	80 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	.....@.....
53:42F0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
53:4300h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....B...
53:4310h:	0E 1F BA 0E 00 B4 09 CD 31 B8 01 4C CD 31 54 68	..*..'.! ,.L!Th
53:4320h:	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
53:4330h:	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
53:4340h:	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode....?.....
53:4350h:	D1 1A D8 4A 95 7B B5 19 95 7B B5 19 95 7B B5 19	\$.0J*(u.*(u.*(u.
53:4360h:	16 67 B8 19 94 7B B5 19 DA 59 BC 19 9A 7B B5 19	.ge."(u.0Y4.8(u.
53:4370h:	A3 5D B9 19 94 7B B5 19 6A 5B B1 19 94 7B B5 19	8).."(u.)(a."(u.
53:4380h:	52 69 63 68 95 7B B5 19 00 00 00 00 00 00 00 00	Rich*(u.....

图6.5 IMG.jpg中的隐写信息

流程A中，携带载荷的图片则使用了RGB值隐写，将恶意代码存放于RGB值的R位：

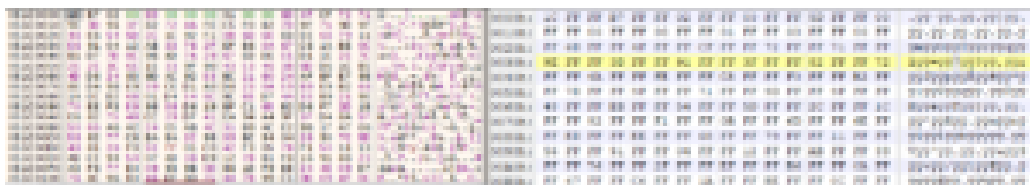


图6.6 隐写图片sKr93l.png中的RGB值（右）与提取到的压缩数据内容（左）

这样的构造使隐写图片在白色区域显示蓝绿色斑点，黑色区域则显示红色斑点：



图6.7 隐写图片sKr93l.png外观



图6.8 隐写图片Fruit.png外观

## 6.4 套接字窗口

本次DarkCasino行动中，Evilnum使用的DarkMe木马使用了SOCKET\_WINDOW通信。

这是一种古老的VisualBasic套接字编程技术，通过一个SOCKET\_WINDOW窗口挂钩winsock消息，并在窗口回调函数中处理由WSAAsyncSelect传递的事件消息。

原始框架可参考：[https://github.com/dzzie/RE\\_Plugins/blob/master/IdaVbScript/vb%20src/MSocketSupport.bas](https://github.com/dzzie/RE_Plugins/blob/master/IdaVbScript/vb%20src/MSocketSupport.bas)

## 6.5 COM组件执行

本次DarkCasino行动中，部分DarkMe木马以COM组件的形式投递。Evilnum攻击者在前置木马载荷中写入注册表操作逻辑，使其可以产生并执行带有如下内容的Register.reg文件：

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B8C7-5244-483E-A0E0-D549E9CEA39E}]
@="ShellRunDllVb.CShellRunDll1"
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B8C7-5244-483E-A0E0-D549E9CEA39E}\ImplementedCategories]
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B8C7-5244-483E-A0E0-D549E9CEA39E}\ImplementedCategories]
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B8C7-5244-483E-A0E0-D549E9CEA39E}\InprocServer32]
@="C:\Users\%1\AppData\Local\update\ShellRunDllVb.dll"
"ThreadedMode"="Apartment"
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B8C7-5244-483E-A0E0-D549E9CEA39E}\ProgID]
@="ShellRunDllVb.CShellRunDll1"
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B8C7-5244-483E-A0E0-D549E9CEA39E}\Programmable]
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B8C7-5244-483E-A0E0-D549E9CEA39E}\TypeLib]
@="{8F1576CB-8889-4F85-87A6-268C8D548794}"
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B8C7-5244-483E-A0E0-D549E9CEA39E}\VERSION]
@="1.0"
```

图6.9 Register.reg文件内容

随后前置木马载荷通过形如rundll /sta [CLSID] 'Hello'的cmd指令启动DarkMe木马。

这样的方式避免了对DarkMe木马的直接调用，一定程度上减少了暴露风险。

## 七、总结

DarkCasino行动是一场正在发生的，针对网络交易现金流的APT攻击活动。Evilnum在该行动中使用了多种经过不断改良的攻击手法和工具，展现了其敏锐的对抗意识。

分析表明，DarkCasino行动的影响范围并不局限于欧洲，在Evilnum攻击者的运营下，本次攻击最终辐射到了部分亚洲国家，有可能造成意料之外的危害。

为有效防范本次APT行动，应尤其注意通过各种渠道传递的LNK、PIF、SCR、COM类型文件，提高对带有offer、visa、casino等关键词的文件的警觉性，避免因Evilnum的网络攻击造成直接经济损失。

## 八、IoCs

攻击流程A诱饵文件

43eda4ff53eef4513716a5b773e6798653ee29544b44a9ae16aa7af160a996f2 offer deal visa 2022.lnk

攻击流程B诱饵文件

5fb252474237a4ca96cc0433451c7d7a847732305d95ceaeab10693ecef2eeee Scatters Casino offers Daily Promotions.pif

8e4a4c5e04ff7ebacb5fe8ff6b27129c13e91a1acc829dbb3001110c84dc8633 new casino crypto.com

d0899cb4b94e66cb8623e823887d87aa7561db0e9cf4028ae3f46a7b599692b9 Promo CPL CPA Traffic.com

攻击流程C诱饵文件

4ffa29dead7f6f7752f2f3b0a83f936f270826d2711a599233dc97e442dee85f 333TER.exe

9cf7f8a93c409dd61d019ca92d8bc43cc9949e244c9080feba5bfc7aac673ac3 d33v3TER.exe

259cebed2cd89da395df2a3588fadde82cd6542bc9ff456890f7ee2087dc43c9 d333TER.exe

0cdf27bb8c0c90fc1d60fb07bd30b7e97b16d15e3f58fb985350091ecad51ba6	ed333TER.exe
5ba84191a873d823ccf336adfa219cc191a004e22b56b99c6d0e1642144129b8	wed333TER.exe
15a076c7bb6a38425d96aa08b8a15e9a838c9697d57c835aaca92fd01607b07a	PayRedeemUpdateIntegration19052022.scr
3329f5e3a67d13bd602dca5bbe8e2d0b5d3b5cb7cb308965fb2599a66668c207	offer crypto casino.scr
8a49a7f6c95fade72ef86455794cdedfca9129aa0f5281e09929dfebf3417c4	DOCUMENTATION AGREEMENTS S CONSULTING INTEGRATION.pif

下载者木马

864dccbeda7d88cad91336b5ae9efd50972508d1d8044226e798d039a0bc1da2 AONNRJP.exe

PikoloRAT木马

eb5e42c726c7b125564455d56a02b9d42672ca061575ff911672b9165e8e309d stub1.exe

be544a1f9f642bb35a9bd0942ae16a7a6e58a323d298a408a00fa4c948e8ea17 Stub1.exe

DarkMe木马

a826570f878def28b027f6e6b2fcd8be1727e82666f8b65175d917144f5d0569 Project1.exe

7b478cd8b854c9046f45f32616e1b0cbdc9436fa078ceddb13ce9891b24b30a5 Project1.exe

e72337c08d6b884b64fd9945c5a01557ccf40db93af866c00c48d36b6605f3a0 Project1.exe

414a11e8eabb64add97a866502edcd7e54108bd247f4ae12fe07feeae4e549f6 Projec3.exe

7913cdf40cc17a28487a71ab0d7724b8bf3646a2a53e3905798ce23a657061b8 Project1.exe

3a6694567e9d722357b8e92153d9c878bbcab55a2f65cd0f9a2e6579fbeb935a Projec3.exe

a6a70c85b8c40932678c413fde202a55fcfc9d9cae23822708be5f28f9d5b6d2 Projec3.exe

c50ebe13972e6e378248d80d53478d8e01e754c5d87113d9b6f93bf3b84380b4 Project1.exe

1ac7715b1762788b5dc1f5f2fc35243a072fe77053df46101ce05413cca62666 Projec3.exe

4ecc2925cfb073323314611a3892d476a58ff2f6b510b434996686e2f0ac3af7 Projec3.exe

541b3011953a3ce1a3a4a22c8c4f58c6a01df786a7cc10858649f8f70ee0a2f3 Projec3.exe

f25cbc53d0cc14b715ee83e51946d5793e4e86e71e96f68e9b6c839b514e8cb8 Projec3.exe

4244f274a12f4672f2dda1190559d96c5a9631c9ee573b853c89e30701819b63 Projec24.pif

1f0d908c677fb3ec5b9422eb5f7d2a2b3ffa01659521afc07cc4dfaea27aa532 Nuovo.pif

028057e54a2e813787a14b7d33e6a2caa91485ed879ef1bbcb94df0e1cf91356 bvo.exe

0a9c183f0b5a225228da5e8589fac8b3affe2e51c790a08148ef72481de610c4 bvo.exe

3eb84676249cb26dd3d1962cfca2a9fde442d0feaa1b0351f6331313f3ac1138 bvo.exe

46fbfc263959084d03bd72c5b6ee643711f79f7d76b391d4a81f95b2d111b44e bvofinal.pif

5e04dd49b82320eca63b483e87453d2a68a9f4873f47d37e5080d537bc811d0e ppppsst.exe

dc8190279dcea4f9a36208ba48b14e6c8313ef061252027ef8110b2d0bd84640 ppppsst.exe

4959cdba7edee68b5116cc1b8ef5016978d3dff2016f027a4f76b080b7c3849a faster.exe

24ace8fd73b2a5a13f3e5b459f0764dd4b5bda2cea2b0e13bbf88a88afe0cdac fastest.exe

c66e6ee55e9799a8a32b7a2c836c26bb7ebea98d09c1535ad9ae59e9628835fb	fastest.exe
32ce8d0dcbfcc2517480d0e08f8896ab4f6ea13ccb0eefe7205cd352c7b359c3	h5a.exe
c192684d296ea587e93457d060cbef900143cf1a11301e6c2e34e264e3e55ef6	h5a.exe
1d01b143a56eba431387b9b973790d174deb48c2e3445d96b131a7d8e0a9d4ef	vvt1.exe
b8ba2c0478649dc099d0a869755a7e205173a9b0d15fad920317a89d07eaa930	vvt1.exe
d95853e6e16d90c00fd72aaeaca9885b953dae14d7d6aa7fedcc6150fb788667	656.exe
7add6700c6e1aa1ac8782fdd26a11283d513302c672e3d62f787572d8ad97a21	ShellRunDIIVb.dll
17fe047b9a3695d4fd8ad9d2f7f37486c0bc85db0f9770471442d31410ff26a1	ShellRunDIIVb.dll
2665a09ec5b4ca913f9f3185df62495f13611831dba9073779a36df088db143b	ShellRunDIIVb.dll
7c06a03d712be8c0df410bea5d1c2004c6247bcde5a46ce51746f18de9621ac1	ShellRunDIIVb.dll

#### URL

<https://puccino.altervista.org/wp-content/uploads/2022/05/6h.txt>

<https://storangefilecloud.vip/IMG.jpg>

<https://storangefilecloud.vip/PI.txt>

<https://storangefilecloud.vip/PRGx.jpg>

<https://bukjut11.com/FRIGO.JPG>

<https://bukjut11.com:443/AEVC.JPG>

<https://imagizer.imageshack.com/img922/1527/sKr93I.png>

<https://imagizer.imageshack.com/img923/7651/jMwIGI.png>

<https://i.imgur.com/fkNiY9Z.png>

<https://laurentprotector.com/LRGBPFV.bin>

<https://laurentprotector.com/NnQFqsOEUtkezviEcLpfa.bin>

#### Darkme CnC

[aka7newmalp23.com](http://aka7newmalp23.com)

[csmmmmsp099q.com](http://csmmmmsp099q.com)

[muasaashishaj.com](http://muasaashishaj.com)

[cspapop110.com](http://cspapop110.com)

[938jss.com](http://938jss.com)

[8as1s2.com](http://8as1s2.com)

[kalpoipolpmi.net](http://kalpoipolpmi.net)

[pallomnareraebrazo.com](http://pallomnareraebrazo.com)

[185.236.231.74](http://185.236.231.74)

#### PikoloRAT CnC

[51.195.57.232](http://51.195.57.232)

## 版权声明

本站“技术博客”所有内容的版权持有者为绿盟科技集团股份有限公司（“绿盟科技”）。作为分享技术资讯的平台，绿盟科技期待与广大用户互动交流，并欢迎在标明出处（绿盟科技-技术博客）及网址的情形下，全文转发。

上述情形之外的任何使用形式，均需提前向绿盟科技（010-68438880-5462）申请版权授权。如擅自使用，绿盟科技保留追责权利。同时，如因擅自使用博客内容引发法律纠纷，由使用者自行承担全部法律责任，与绿盟科技无关。