Operation DarkCasino: In-Depth Analysis of Attacks by APT Group Evilnum (Part 1) - NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks.

By NSFOCUS

Published: 2022-09-19 · Archived: 2026-04-05 14:54:52 UTC

Overview

Recently, NSFOCUS Security Labs observed a series of phishing activities against European countries. Those activities mainly targeted online gambling platforms as well as active online trading behaviors, aiming to steal transaction credentials of service providers and customers for illegal profits.

The in-depth analysis revealed that it was a continuation of recent attacks staged by the ATP group Evilnum. Evilnum attackers followed their typical attack methods in this operation. Compared with previous activities, this operation adopted more diversified attack flows and more complicated attack components and used two new trojans, DarkMe and PikoloRAT, demonstrating its high tool development ability, flow design ability, and rich experience in offensive and defensive confrontation. It was also observed that Evilnum's design methods and implementations varied significantly in different attack flows, so the researchers believed that multiple attackers took part in this operation.

NSFOCUS Security Labs named this operation DarkCasino based on its attack targets and trojan programs. This operation showed that the Evilnum group still took online trading platforms as their prime targets. The group could rapidly find cybercrime opportunities and then take actions.

Until the release of this report, the DarkCasino operation is still in progress.

About APT Group Evilnum

First spotted in 2018, the Evilnum group has been active in the UK and Europe, whose key targets are financial technology companies. The group is named after the Evilnum trojan, also called DeathStalker by Kaspersky Lab.

The goal is to steal transaction credentials to gain control of the company or individual accounts for theft of funds.

Evilnum's typical attack method is to disguise malware as the client identity file to trick Fintech staff into running the program. Then the embedded spy trojans will steal high-value information from victim hosts.

The Evilnum group has strong development abilities to design complicated attack flows and components. NSFOCUS Security Labs had ever observed and disclosed that Evilnum's attack flows were launched with a high completion rate and a stub trojan, AgentVX, was used.

Attacked Targets

NSFOCUS's analysis revealed that most victims of this operation were in European countries in the Mediterranean region. Attacks were also observed in Canada, Singapore, and the Philippines. Its direct targets include online gambling platforms, consumers in various countries using such media, and other personnel related to online transactions on the platform.

The identified attack flows showed that Evilnum used the following character strings as the decoy file name.

Decoy File Name
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

Scatters Casino mentioned above is an online casino operated by Gammix Limited, a Maltese company. Decoy files were disguised as online transaction credentials or promotion files to attack Scatters's operations staff, and they were also disguised as Scatters's promotion ads to attack customers. Evilnum attackers aimed to steal the transaction credentials and related information stored on target hosts.

The statistics on the source of the decoy files revealed that victims were widely distributed in European countries, such as Malta, Poland, Cyprus, Armenia, Spain, Switzerland, France, and Ireland, as well as in non-European countries such as Canada, Israel, even Singapore, and the Philippines.

Distribution of victims in Operation DarkCasino

In terms of geolocations, many victims were in Malta and a small number of victims were distributed in other countries where Scatters's services are available.

Scatters Casino was launched to the market in 2019 and has expanded rapidly. Recently, Scatters announced that its online casino service had a prize pool of 230 million euros, which may be the leading cause for being targeted by the Evilnum group.

Other information indicated that DarkCasino may be only part of a more persistent, larger-scale attack campaign. Correlation of IoC clues demonstrated that part of Evilnum's assets could be linked to cyberattack activities targeting cryptocurrency-related trading platforms, which started in the second half of 2021 and continued to early 2022. In this operation, large numbers of signed trojans, ParallaxRAT and NetWire, were delivered to steal information from target hosts mainly in Europe. Although the decoys and network resources used by attackers were associated with DarkCasino, NSFOCUS Security Labs did not obtain direct evidence to prove the Evilnum group staged this operation.

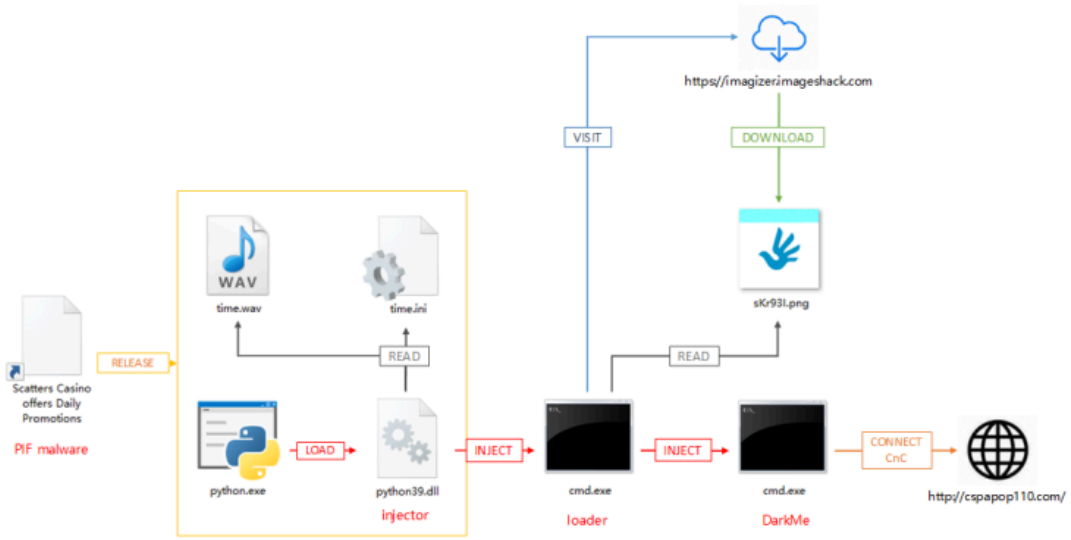
Attack Flows

Evilnum attackers constructed three different attack flows in this operation. All these flows started from sending decoy files. The next step was to access public resources or compromised websites to obtain steganographic images. DarkMe payloads were then extracted from these images and finally loaded and executed in one way or another.

- **Attack Flow A**

As the first attack flow used by Evilnum attackers, it featured the most complicated components. Its key components were first spotted on May 2.

The analysis of components revealed that this attack flow had two variations. Flow A1 was constructed on April 28, which required downloading contents from specific network locations. Flow A2 was constructed on May 1, which did not require downloading content from the network. The two variations had a similar execution process.



DarkCasino attack flow – 1

As shown in the figure above, attack flow A was very similar to that in Operation AgentVX observed and disclosed earlier by NSFOCUS Security Labs. It consisted of the installer generated by InstallShield, side loader, encrypted shellcode loader, steganographic images, and DarkMe trojan.

After InstallShield disguised as a PIF file was started, the generated installer would perform a general installation process, dropping built-in files in the **%TEMP%** system directory and running the legitimate program python.exe.

After python.exe was started, python39.dll carrying malicious code was sideloaded, leading to executing a piece of shellcode in python39.dll.

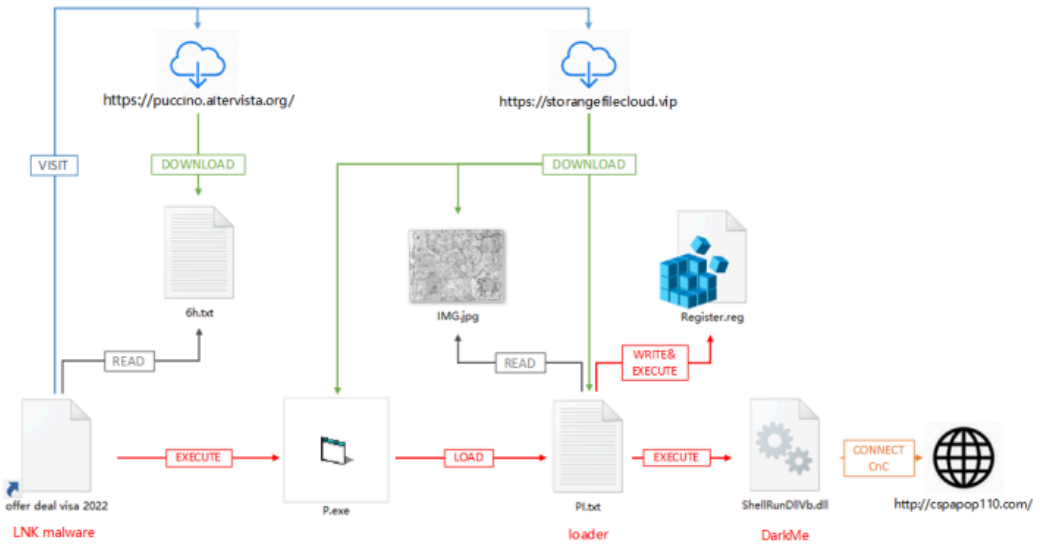
The malicious shellcode in python39.dll read the **time.wav** file in the same directory, decrypted and extracted the next-stage shellcode code, then started the **cmd.exe** puppet process, and injected the next-stage shellcode into it. During the injection, an URL string read from **time.ini** was written to cmd.exe as the startup parameter of the shellcode.

The shellcode in the **cmd.exe** puppet process would obtain a steganographic image from the preceding URL, extract the third-stage shellcode from the image through the built-in image processing module, and execute it.

The third-stage shellcode would try to inject the built-in trojan DarkMe into another puppet process **cmd.exe** and run it. The C&C communication server with which DarkMe communicated was cspapop110.com.

- **Attack Flow B**

This attack flow was first observed on May 9, and related documents showed that the flow was constructed on May 3.



DarkCasino attack flow B

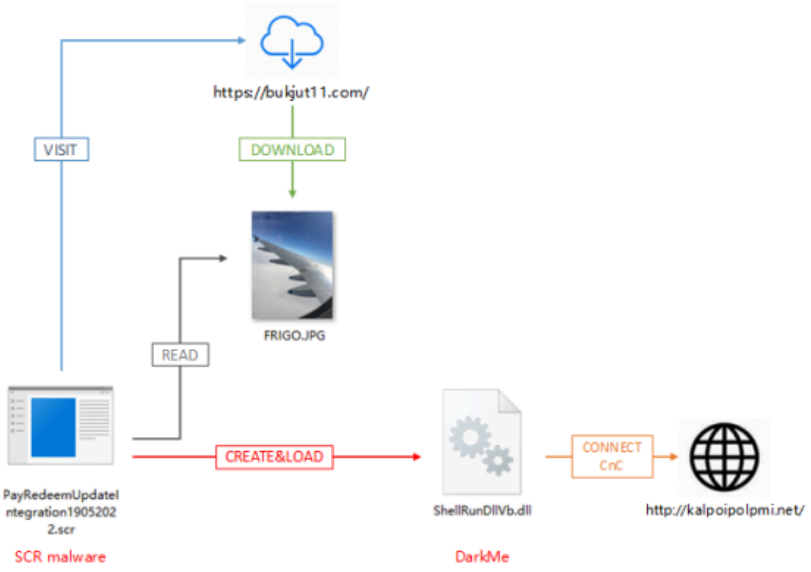
As shown in the figure above, attackers also followed the Evilnum group's common practice in attack flow B. They delivered shortcut decoy files with a malicious **mshta** command, accessed the controlled WordPress website for obtaining the subsequent instruction code, and then ran it.

The key to this flow was to obtain three files **P.exe**, **PI.txt** and **IMG.jpg** by visiting the second-stage site. After being loaded by **P.exe**, the main loader trojan **PI.txt** would extract the hidden executable file ShellRunDllVb.dll from **IMG.jpg**, and register the DLL file as a system component {A762B0C7 -5244-4B3E-ADED-D549E9CEA39E} by creating a registry file **Register.reg**. Then **Pi.txt** ran the **rundll32 /sta** command to execute the component.

Finally, a spy trojan DarkMe was executed, and communicated with the C&C server cspapop110.com.

- **Attack Flow C**

The Evilnum attackers added a more streamlined flow on May 19.



DarkCasino attack flow C

As shown in the figure above, attack flow C was initiated by a loader trojan disguised as an SCR file. The trojan obtained a steganographic image by directly accessing the built-in URL link, extracted the file ShellRunDllVb.dll from the image, and then loaded and executed it. ShellRunDllVb.dll was also a DarkMe trojan, and kalpoipolpmi.net was used as the C&C communication server.

(To be continued…)

Source: https://nsfocusglobal.com/operation-darkcasino-in-depth-analysis-of-attacks-by-apt-group-evilnum-part-1/