



ZEROFOX[®]

Your Intelligence Digest

**It's a Digital World.
Engage Securely.**

New Service Weaponizes Word Documents Using Remote Template Injection

Untested threat actor, “SandboxEvader”, advertised a new service to weaponize Microsoft Word documents, on the Russian language Deep Web forum xss[.]is. Unlike similar services that leverage malicious macros, the actor claims that their service uses a remote template injection to avoid being detected as malicious by most commercial antivirus products and email filters, including Gmail. According to the actor, this injection method involves using a macro-free .docx file that references remotely hosted .dotm template files containing malware or loader. The actor specified that each weaponized document can be customized to execute a threat actor’s own payload.

The actor charged \$125 USD per build. They also claimed to offer discounts on bulk orders.

If the threat actor is legitimate, ZeroFox researchers note that this service could provide threat actors with a new method to gain initial access to systems running Windows, in addition to other malicious purposes.

Remote Template Injection | .DOCX | BYPASS GMAIL

SandboxEvader · 16.04.2022

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧЕСКИЙ

Новая сценка



SandboxEvader

CD-диск

Пользователь

Регистрация: 03.12.2021

Сообщения: 14

Реакции: 6

Гарант сделки: 2

Депозит: 0.0182 B

16.04.2022

Document macros have been around for a long time and have really been overused. Just dropping a malicious .doc rarely works anymore.

- Most AV products detect .doc macros
- .doc with macro code CAN NEVER BE ATTACHED TO GMAIL (even with only a hello world non malicious code)
- A lot of other email scanners outright block .doc with macro code
- Same applies to the Excel macro equivalent

So what can we do now? One of the modern solutions is remote template injection.

Remote Template Injection:

Remote template injection is the improved method over the old malicious .doc. It relies on using "benign" .docx files which can not contain any macro code and as such are considered safe. However, they can reference remote .dotm files which are hosted on a remote server. So the .docx file is just a stager with no malicious code at all and as such it bypasses all AV and email scanners. The only way a .docx file can be that point it is already far too late.

Onto the service description:

I am selling the .docx by the bin.

Both the .docx and the remote code are custom made for each buyer.

All you need to do is supply the direct link to the .exe to be executed. Of course the detection rate of your payload will influence the final success rate.

If somebody wants a specialized build - UAC bypass etc feel free to contact me. I will try to offer the best support that I can!

The price per .docx build is \$125

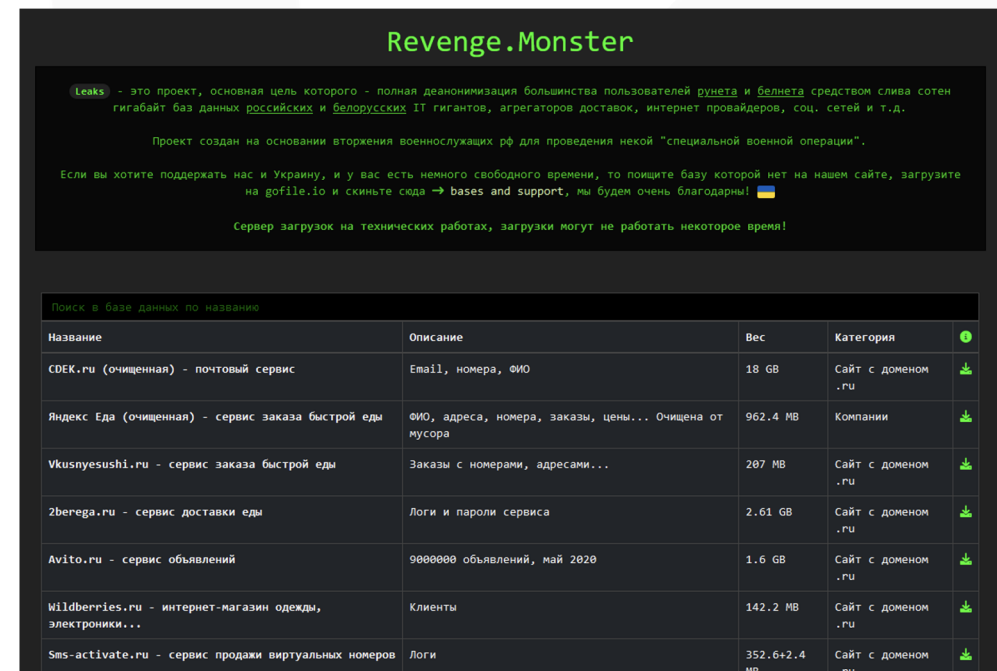
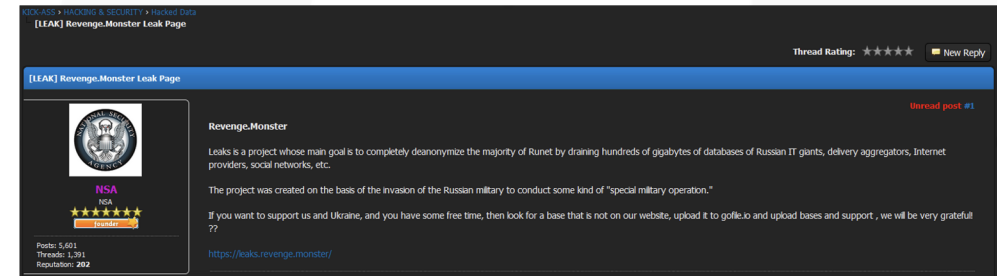
New Aggregator Site Provides Central Hub For Russian-Related Data Leaks

Well-regarded threat actor and administrator “NSA” advertised a new aggregator website, providing a central hub for threat actors to share Russian-related data leaks, on the English language Dark Web forum “KickAss”. ZeroFox researchers note that unlike most threat actors sharing Russian-related leaks on the underground, the developers of this new site, revenge[.]monster, appear to be native Russian speakers. The site features dozens of leaks of Russian-based IT infrastructure companies that have been shared to different Deep Web forums since the start of the Russia/Ukraine war in late February 2022.

According to “NSA”, the goal of this new site is to deanonymize the Russian Internet (AKA runet) by leaking sensitive data related to Russian-based IT companies, including:

- Third-party food delivery aggregators
- Internet providers
- Social networks

The actor is encouraging any pro-Ukrainian forum members to upload new leaks to the site in support of the project.

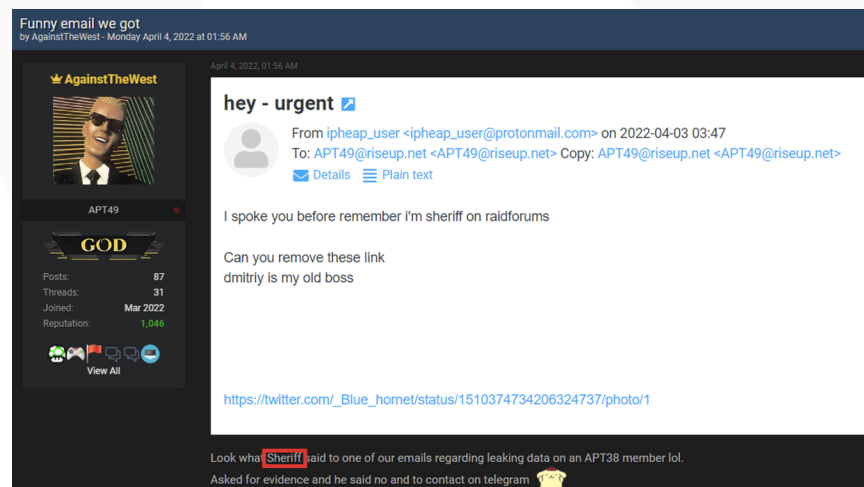
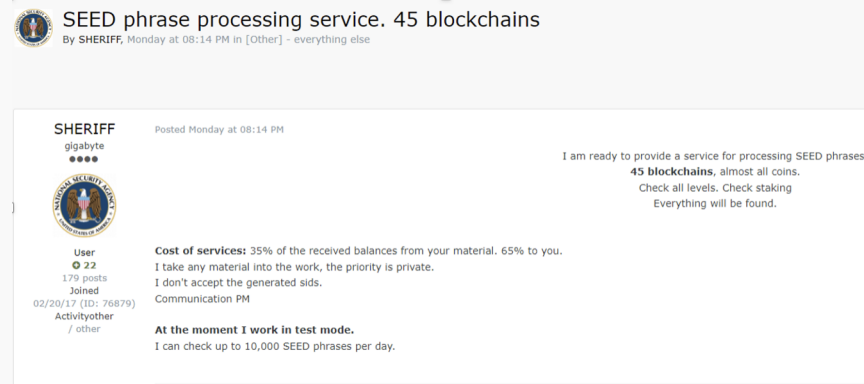


Service Leverages Seed Recovery Phrases To Compromise Crypto Wallets

Well-regarded threat actor “SHERIFF” advertised their new service leveraging seed recovery phrases to compromise cryptocurrency wallets on the Russian language Deep Web forum exploit[.]in. The actor claims that customers can provide them with seed phrases to check against cryptocurrency wallets on 45 different blockchains. If the actor is successfully able to rebuild a victim’s crypto wallet by using the seed phrases, the actor claims that they will drain the wallet and split the funds 35-65 with the customer.

The service has already received positive feedback from threat actors on the forum, including the well-regarded and prominent Russian-speaking threat actor “stallman”.

ZeroFox researchers note that a threat actor with the same alias, “Sheriff”, was recently banned from the English language Deep Web forum breached[.]co. This allegedly happened because the actor was outed by the pro-Ukrainian hacktivist group “AgainstTheWest” for claiming that they previously worked for Dmitry Badin (AKA “Dmitriy Makarov”); a suspected member of the Russian hacker group “Fancy Bear” (AKA “APT28”).



New Version of Spectre RAT Advertised

Well-regarded threat actor “DigitalMutant” advertised a new version of the widely popular Spectre remote access trojan (RAT), on the English language Deep Web forum CryptBB[.]com. The malware contains standard features for a RAT, including a file stealer, a loader, and remote control of a victim’s machine via HVNC.

Additional features for this new version of the RAT include:

- Coded from scratch from C++
- Abuses task scheduler to maintain persistence
- Does not contain software dependencies
- Executes malware at startup
- Provides additional statistics for compromised devices
- Does not decrypt strings all at once
- Gathers cookies in JSON and Netscape formats
- Deletes binary after killing malicious process
- Launches hidden command prompt

The actor charged \$250 USD per month for the RAT. They also offered a preconfigured command-and-control (C2) server for an additional \$50 USD per month.

