



ZEROFOX[®]

Your Intelligence Digest

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

Threat Actor Selling Source Code For Ransomware Project

Moderately credible threat actor “udp” advertised the multi-functional malware, dubbed “Light Locker,” that can generate obfuscated payloads and encrypt whole disks on target machines, on the Russian language Dark Web forum “RAMP.” Researchers highlight this uncommon tactic because most ransomware developers offer an affiliate program, which tend to be more lucrative for developers long-term than selling the source code for their projects outright.

According to the actor, the malware mimics other programs on victim machines and triggers the User Account Control (UAC) to execute payloads with elevated privileges. This increases the likelihood of compromising a target machine, as privileges are escalated without the victim’s knowledge, elevates for a seemingly legitimate program on their machine.

Additional features of the malware include:

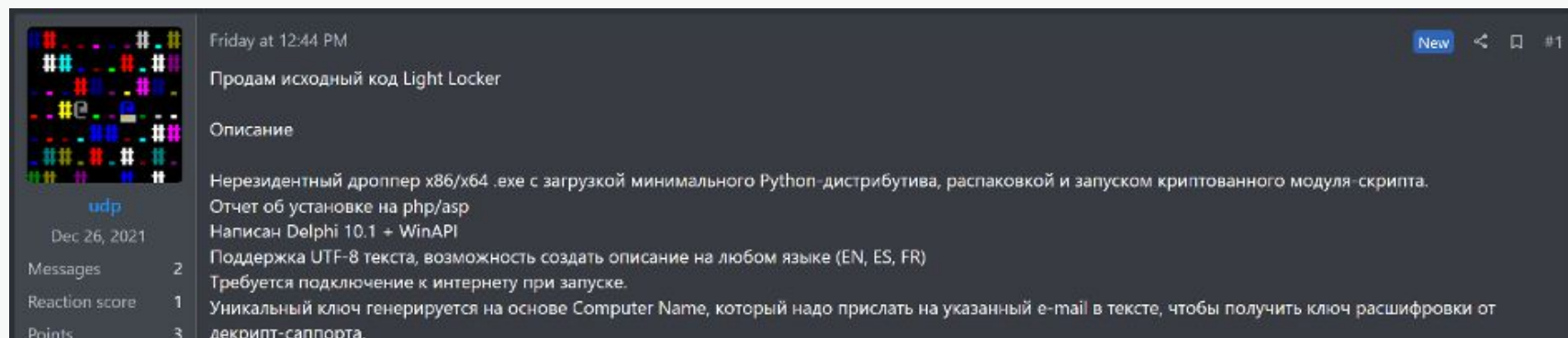
- Works on machines running Windows 7 or 10 (32/64-bit architectures)
- Fast build time (less than 3 minutes)
- Written with Delphi 10.1 Berlin and WinAPI
- Will not be detected as malicious by UAC or SmartScreen
- Exploits SMB to spread through corporate networks

The actor charged USD \$2,000 for the source code. The actor stated that they plan to sell multiple copies.

ZeroFox researchers assess that the sale of this project could potentially lead to the proliferation of new ransomware groups, since the actor is selling the malware outright.

Original post from threat actor “udp” advertising the source code for their ransomware project.

Threat Actor Selling Source Code For Ransomware Project (Cont.)



Friday at 12:44 PM

New < □ #1

Продам исходный код Light Locker

Описание

Нерезидентный дроппер x86/x64 .exe с загрузкой минимального Python-дистрибутива, распаковкой и запуском криптованного модуля-скрипта.
Отчет об установке на php/asp
Написан Delphi 10.1 + WinAPI
Поддержка UTF-8 текста, возможность создать описание на любом языке (EN, ES, FR)
Требуется подключение к интернету при запуске.
Уникальный ключ генерируется на основе Computer Name, который надо прислать на указанный e-mail в тексте, чтобы получить ключ расшифровки от дешифр-суппорта.

udp
Dec 26, 2021

Messages	2
Reaction score	1
Points	3

16 Zero-Day Exploits For Vulnerabilities In WooCommerce Plugin Advertised

New and positively trending threat actor “nixploiter” advertised 16 independent, alleged zero-day exploits for vulnerabilities in a WordPress e-commerce plugin, known as WooCommerce, on the Russian language Deep Web forum “Exploit.” Some of the alleged vulnerabilities include:

- Stored cross-site scripting (XSS)
- Remote code execution (RCE)
- SQL injection
- PHP file upload
- Arbitrary options update

The actor claims that none of the exploits require administrator privileges to run.

If found to be legitimate, ZeroFox researchers expect a significant increase in cyber-attacks against e-commerce sites built using WordPress in conjunction with WooCommerce. Currently, more than 3.8 million websites are leveraging the plugin worldwide.

Pricing per exploit starts at USD \$1,000.



Wocommerce premium plugin 0days

By nixploiter, Friday at 09:14 AM in [Software] - malware, exploits, bundles, crypts

nixploiter

byte



Paid registration
2

11 posts

Joined
07/11/22 (ID: 133155)

Activity
хакинг / hacking

Deposit
0.005000 \$

Posted Friday at 09:14 AM (edited)

I have bunch of wocommerce premium plugins 0day exploits (16).

All unknown vulnerabilities and no patches, requires no admin privileges.

Available vulnerabilities:
Stored XSS, RCE, SQL injection, PHP File upload, arbitrary option update.

Price: 1000\$+ each.

If interested contact me by PM.

Edited Friday at 09:20 AM by nixploiter

Actor Shares Method To Create Botnets

New and positively trending threat actor “Nu11B17” (AKA “Nullbit”) shared a method they claim threat actors can use to create their own botnets, on the English language Dark Web forum “CryptBB.” The method involves using compromised student email accounts to register for Shodan accounts, giving threat actors access to the Shodan command-line-interface (CLI).

Individuals may then leverage the Shodan CLI with the Nuclei scanner templates to scan and identify devices with known security flaws or vulnerabilities. The actor claims that they successfully compromised over 10,000 devices using this method to mine cryptocurrency and perform distributed denial-of-service (DDoS) attacks.

The actor previously advertised more than 500,000 compromised student email accounts from 15 universities, along with the SQL injection method allegedly used to secure this data.

The actor charged USD \$1.50 per student email account, with a minimum of 20 accounts per order.

Original post from threat actor "Nu11B17", who shared a new method they claim threat actors can use to create their own botnets.

Actor Shares Method To Create Botnets (Cont.)

1.5m shodan member account



Nu11B17 •
Member
Member

Posts: 26
Joined: Jul 2022
Reputation: 4

#1

07-23-2022, 05:34 PM

„Hello It's Nu11BI7
Want To Scan the world With Me?

i assume u already know what is shodan , if not google it and come back ,
YOU KNOW as iam selling own leaked db from .edu mails , i use them also to get membership at Shodan it costs for non-student (50\$) [/showthread.php?tid=9399&pid=29855#pid29855]
but for me it costs time ,for you it only costs 1.5\$/mail (min 20 mail) YOU JUST SAVED 48.5\$/1MAIL
You are Lazy being signup in outlook and don't have access to phone number ? i can do it for you dude 😊
So what benefices from shodan ?
u can check this thread to how make zombies from shodan api [/showthread.php?tid=9401]

Uptick in sale of initial access to Italian-based companies

On 23 July 2022, ZeroFox researchers observed positively trending threat actor “Insider Inc” announce that they are able to exfiltrate data from several U.S. companies via a network of insiders, on the Deep Web, predominantly Russian language forum WWH-Club. The threat actor did not identify the targeted companies by name but claimed they were “worth attention.” On 1 August 2022, the threat actor updated this thread with a link to a Telegram channel containing more information about initial accesses. The title of the thread indicates that the actor also possesses insiders in European-based companies but made no reference to this in their posts.

The threat actor presents a unique threat to the alleged entities as they could easily sell exfiltrated data procured from insiders, sell the initial network access to a different threat actor/group to conduct secondary attacks (i.e. Ransomware or Data kidnapping attacks), or conduct other malicious activities.

Insider Inc | Private buyout of corporate information in the US and Europe
Insider Inc · 23 Jul 2022



Insider
Insider Inc
Observer
Project participant

Sign up: 31 Jul 2021
Messages: 22
Reaction: 3
General Sales: \$0
General Purchases: \$843

23 Jul 2022
Only the best corporate access to American top corporations. Each lot is worth its attention
https://t.me/Insider_Inc



Insider
Insider Inc
Observer
Project participant

Sign up: 31 Jul 2021
Messages: 22
Reaction: 3
General Sales: \$0
General Purchases: \$843

Today at 09:34
Over time, I will publish information about the scale and levels of network access
https://t.me/Insider_Inc