



ZEROFOX®

Your Intelligence Digest

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

New Ransomware-As-A-Service Project Established

Untested threat actor “cobaltforce” announced a newly established ransomware-as-a-service (RaaS) project on the predominantly Russian language Dark Web forum “RAMP”. Unlike similar services, this new, unnamed project automates most interactions between the affiliate groups and ransomware developers, giving affiliates more autonomy to run the campaigns. The project is designed to compromise devices running various operating systems and software that creates and runs virtual machines, including:

- Windows
- Linux
- VMWare ESXi

Additional features of the project include:

- Strong encryption
- Leverages multithreading to encrypt files faster
- Performs directory traversal attacks to gain access to sensitive files
- Generates new Cobalt Strike payloads via remote server
- Moves through multiple systems on the network
- Encrypts hidden drives

ZeroFox researchers assess this new project is likely to attract a significant number of affiliates because they would immediately have an elevated role within the ransomware gang.

Original post from threat actor "cobaltforce" announcing a newly established ransomware-as-a-service (RaaS) project

New Ransomware-As-A-Service Project Established (Cont.)



cobaltforce
Feb 21, 2022

Messages 1
Reaction score 0
Points 1

Wednesday at 12:17 PM

Windows, Linux & ESXi Affiliate Program

Веб панель:

Крипт:
Функция криптования на лету полезной нагрузки CobaltStrike, а так же максимальное поддержание чистоты создаваемых билдов, генерация билдов и крипт полезных нагрузок производится на удаленном сервере, веб панель не хранит у себя билды шифрования и расшифровки.

Хранилище:
Всем партнерам предоставляется хранилище по протоколу webdav

Командная работа:
Спец роль (Супервизор) в панели позволит вам регистрировать staff персонал, и назначать доступ и уровни доступа к тем или иным кампаниям, вы можете создать неограниченное кол-во групп, люди в рамках одной группы могут общаться в чате между собой, вы можете определить какие кампании видит группа, какие не видит, так же есть возможность, ограничить группу режимом только просмотр и запретить любые функциональные действия в панели в рамках данной кампании. staff персонал не может самостоятельно создавать кампании, создание кампаний и финансовые потоки остаются в полном контроле Супервизора.

Кампания:
После создания кампании вам доступно создание билдов, а так же создание ребилдов на лету, если предыдущий билд вас не устроил по каким то причинам. Кол-во ребилдов ограничено, но лимит всегда можно расширить через Администратора. При первом создании билда вам будет предложено внести изменения в записку, это можно сделать только при первичном создании, и в рамках приличия, никаких сторонних контактов и так далее, все как у всех.

New

< > #1

Data Breach Impacting Stockpile Announced

Well-regarded threat actor “nightly” announced a data breach impacting Stockpile, the digital brokerage, on the predominantly Russian language Deep Web forum “XSS”. The actor claims the breach involves the PII of more than one-million users, along with an undisclosed number of gift cards that contain stock shares or cryptocurrency. Compromised data includes a user’s:

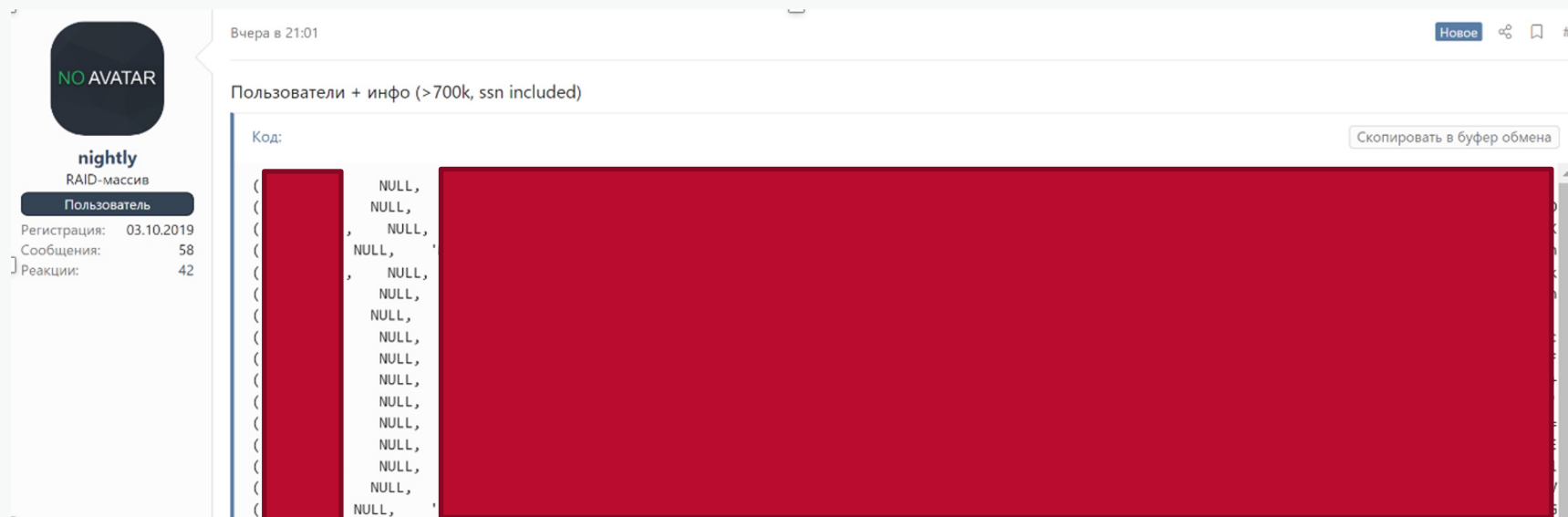
- Full name
- Email address
- Hashed password
- Gender
- Date of birth
- SSN

The actor charged \$75,000 USD for the complete dataset. They also agreed to use an escrow service, indicating the actor is more likely to possess what they claim.

ZeroFox researchers assess that it is virtually certain a threat actor can resell the stolen data or cash out funds from the gift cards to turn a profit on the criminal underground, due to the constant demand among both vendors and threat actors for fresh sets of PII and gift cards.

Original post from threat actor "nightly" announcing a data breach impacting Stockpile

Data Breach Involving Stockpile Announced (Cont.)



Вчера в 21:01

Новое 🔊 📌 #1

nightly
RAID-массив
Пользователь

Регистрация: 03.10.2019
Сообщения: 58
Реакции: 42

Пользователи + инфо (>700k, ssn included)

Код: Скопировать в буфер обмена

(	NULL,	
(	NULL,	
(	, NULL,	
(	NULL,	
(	, NULL,	
(	NULL,	
(	NULL,	
(	NULL,	
(	NULL,	
(	NULL,	
(	NULL,	
(	NULL,	
(	NULL,	
(	NULL,	
(	NULL,	
(	NULL,	
(	NULL,	
(	NULL,	
(	NULL,	
(	NULL,	
(	NULL,	

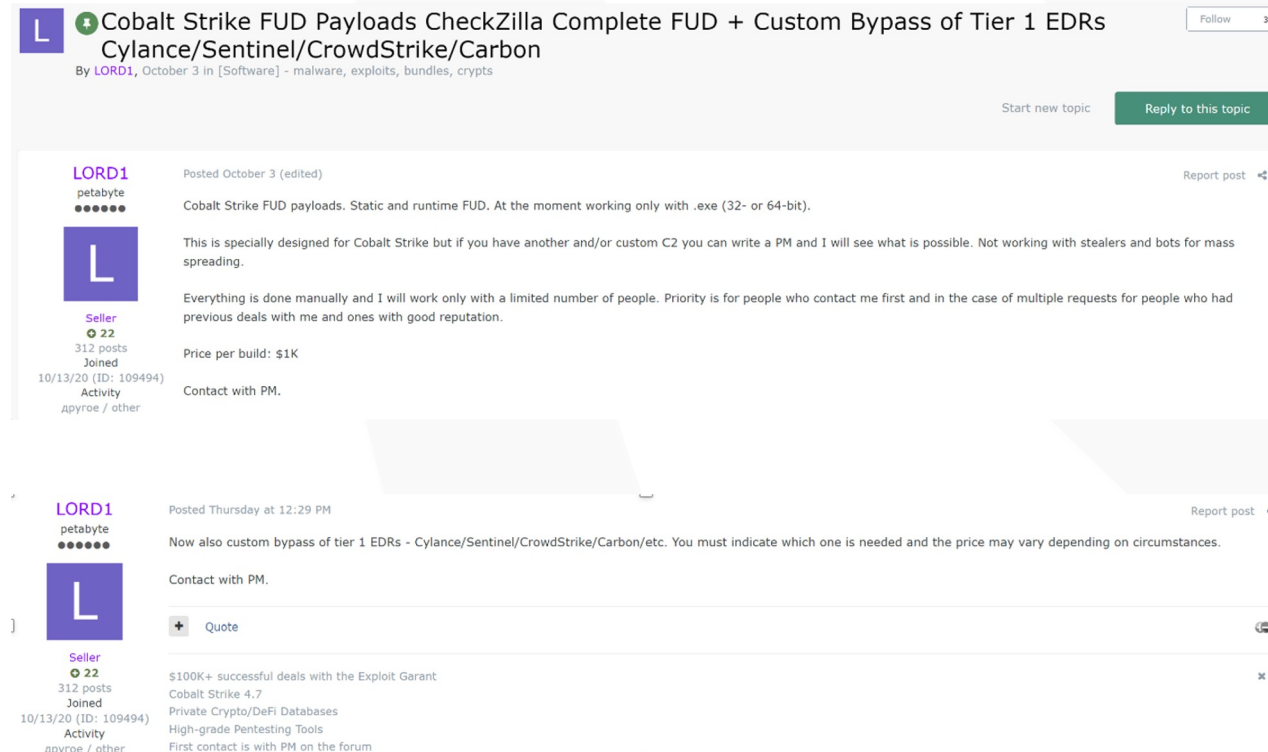
Custom Payloads That Avoid Detection By EDR Solutions Advertised

Well-regarded threat actor “LORD1” advertised a service to generate custom Cobalt Strike payloads that will not be detected as malicious by multiple Endpoint Detection and Response (EDR) solutions on the predominantly Russian language Deep Web forum “Exploit”. The announcement follows a recent trend where an increasing number of threat actors are developing methods to bypass EDR solutions to compromise corporate targets. The impacted EDR solutions allegedly include:

- Cylance
- SentinelOne
- CrowdStrike
- Carbon Black

The actor said that each payload is customized based on the target and the goals of the threat actor. They claim to build 32-bit or 64-bit executable files.

Prices for the payloads start at more than \$1,000 USD per build.



LORD1 petabyte
Seller
22
312 posts
Joined
10/13/20 (ID: 109494)
Activity
apryoe / other

Cobalt Strike FUD Payloads CheckZilla Complete FUD + Custom Bypass of Tier 1 EDRs
Cylance/Sentinel/CrowdStrike/Carbon
By LORD1, October 3 in [Software] - malware, exploits, bundles, crypts

Follow 3

Start new topic Reply to this topic

Posted October 3 (edited)

Cobalt Strike FUD payloads. Static and runtime FUD. At the moment working only with .exe (32- or 64-bit).

This is specially designed for Cobalt Strike but if you have another and/or custom C2 you can write a PM and I will see what is possible. Not working with stealers and bots for mass spreading.

Everything is done manually and I will work only with a limited number of people. Priority is for people who contact me first and in the case of multiple requests for people who had previous deals with me and ones with good reputation.

Price per build: \$1K

Contact with PM.

Report post

Posted Thursday at 12:29 PM

Now also custom bypass of tier 1 EDRs - Cylance/Sentinel/CrowdStrike/Carbon/etc. You must indicate which one is needed and the price may vary depending on circumstances.

Contact with PM.

Quote

\$100K+ successful deals with the Exploit Garant
Cobalt Strike 4.7
Private Crypto/DeFi Databases
High-grade Pentesting Tools
First contact is with PM on the forum

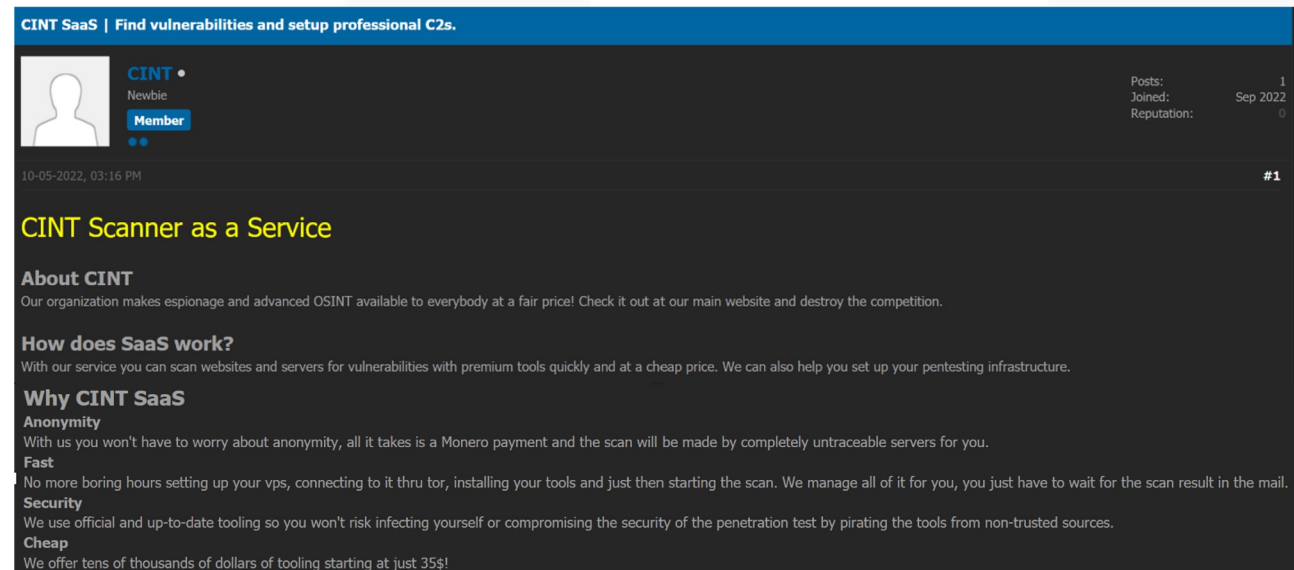
Service Provides Threat Actors With Access To Various Penetration Testing Tools

New and untested threat actor “CINT” advertised a service to scan target networks for potential vulnerabilities, dubbed “CINT Scanner as a Service”, on the English language Dark Web forum “CryptBB”. The service provides users with access to a comprehensive set of premium penetration testing tools, including:

- Metasploit Professional
- Invicti Enterprise
- Acunetix
- Burp Suite Enterprise
- Cobalt Strike
- Brute Ratel

The actor charged \$35 USD for a single scan using most tools. There was also an option to perform an unlimited number of scans for \$100 USD per month.

ZeroFox researchers assess this service is highly likely to succeed because it allows threat actors to quickly begin reconnaissance on a target without having to buy expensive licenses or rely on compromised (AKA cracked) versions of software.



CINT SaaS | Find vulnerabilities and setup professional C2s.

CINT • Newbie Member

10-05-2022, 03:16 PM #1

CINT Scanner as a Service

About CINT

Our organization makes espionage and advanced OSINT available to everybody at a fair price! Check it out at our main website and destroy the competition.

How does SaaS work?

With our service you can scan websites and servers for vulnerabilities with premium tools quickly and at a cheap price. We can also help you set up your pentesting infrastructure.

Why CINT SaaS

Anonymity
With us you won't have to worry about anonymity, all it takes is a Monero payment and the scan will be made by completely untraceable servers for you.

Fast
No more boring hours setting up your vps, connecting to it thru tor, installing your tools and just then starting the scan. We manage all of it for you, you just have to wait for the scan result in the mail.

Security
We use official and up-to-date tooling so you won't risk infecting yourself or compromising the security of the penetration test by pirating the tools from non-trusted sources.

Cheap
We offer tens of thousands of dollars of tooling starting at just 35\$!