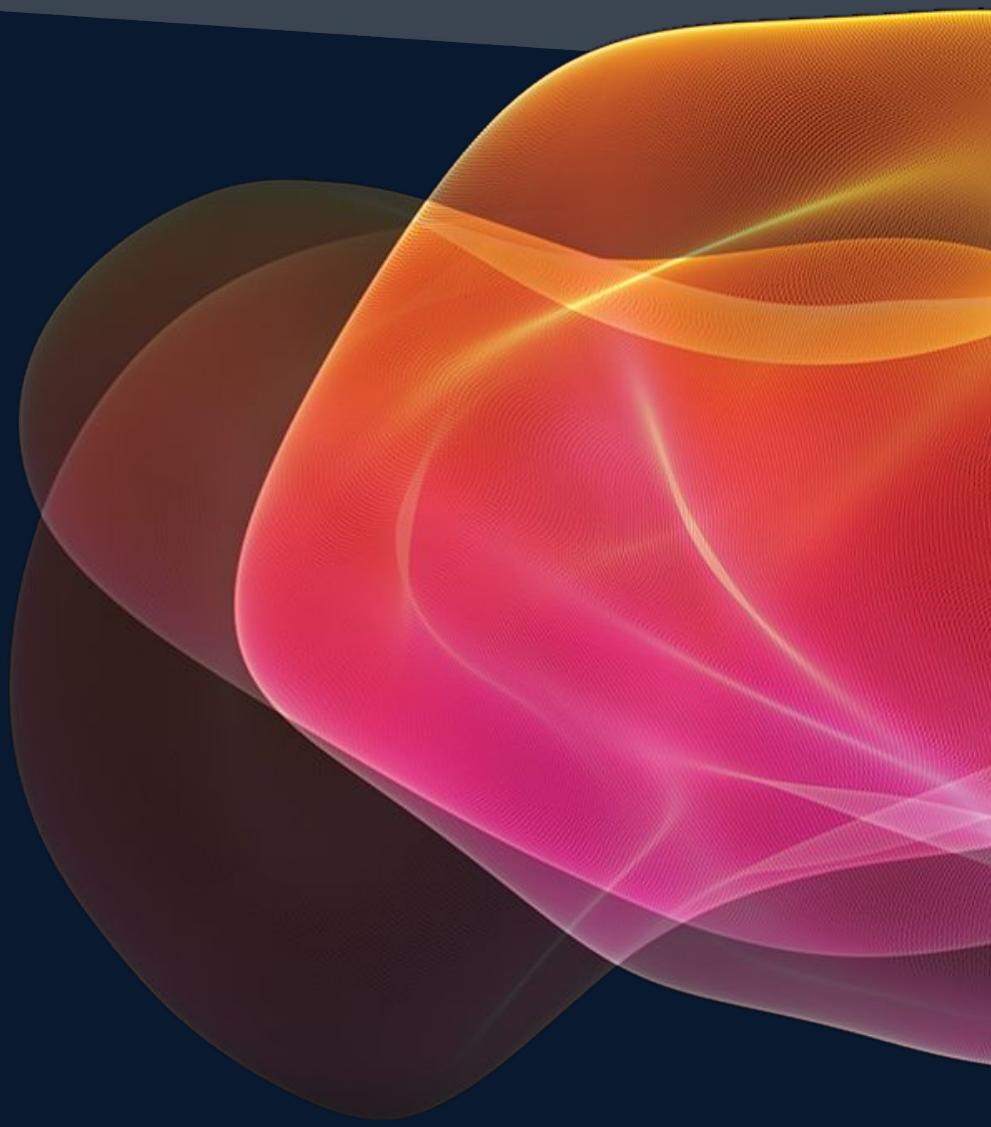
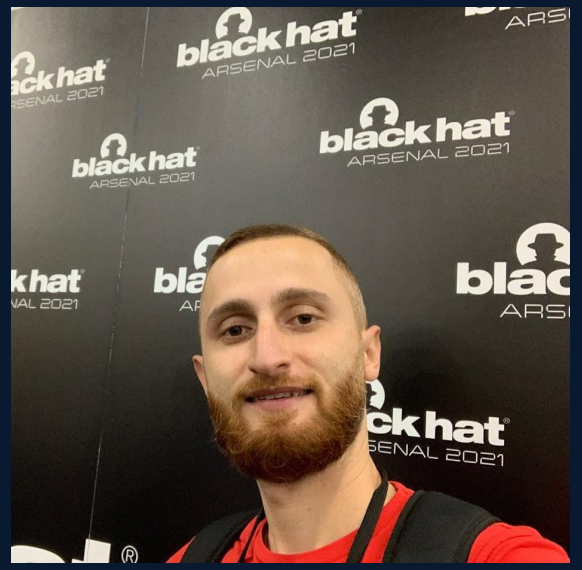
From simple log to sophisticated crypter

Arnold Osipov & Hido Cohen



About Us

Arnold Osipov



Malware Researcher **@Morphisec**

B.S.c Software Engineering

@osipov_ar

Hido Cohen

Malware Researcher **@Morphisec**

B.S.c Communication Systems Engineering

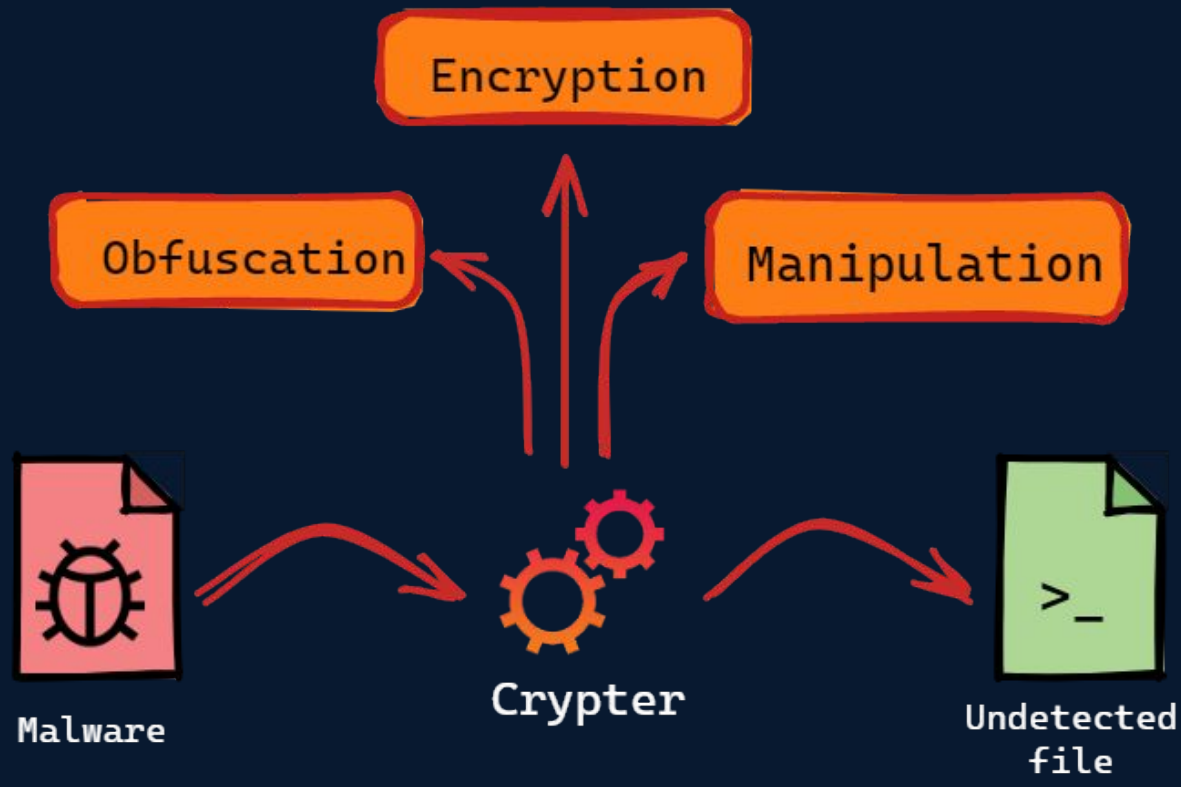
@0xhido

Agenda

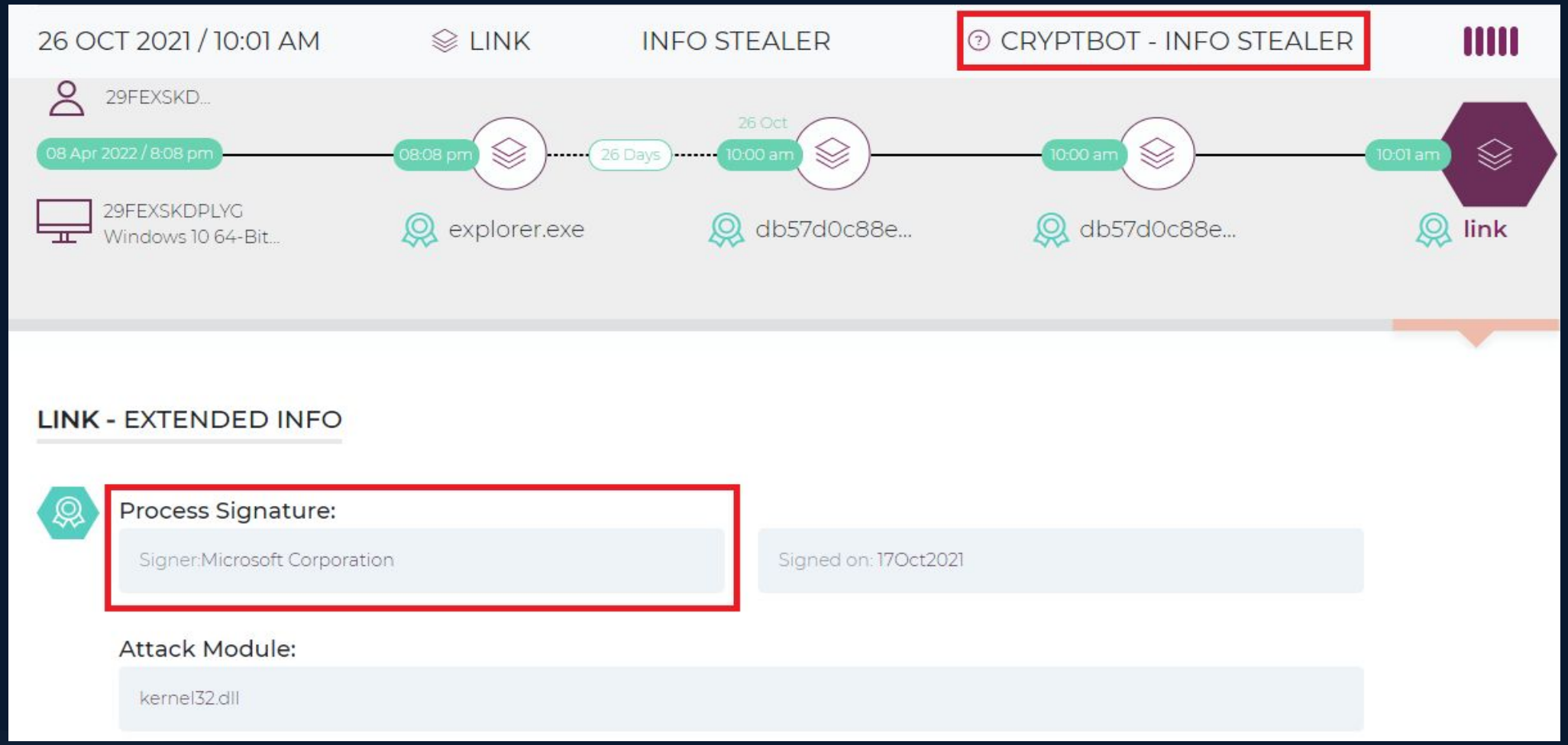
- Encountering an Unknown Crypter
- The Crypter’s Internals
- Hunting The Crypter’s Uses:
  - NFT Campaign
  - Babadeda Against Ukraine
- Summary and Q&A

What a Crypter is?

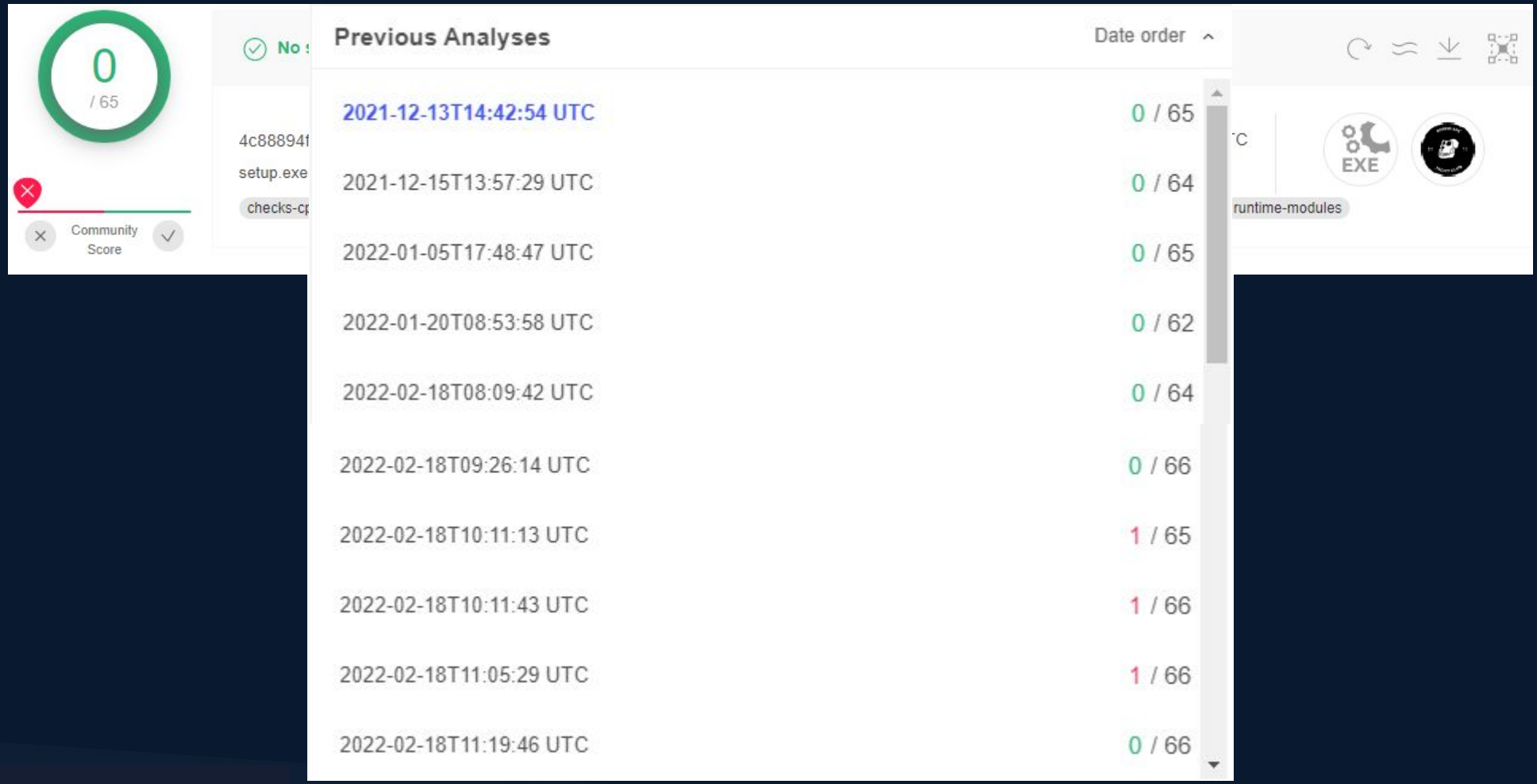
- A program whose goal is to hide the real intentions of a piece of code.
- It does so by using:
  - Encryption
  - Obfuscation
  - Execution manipulation
  - More ...



The Story Begins With



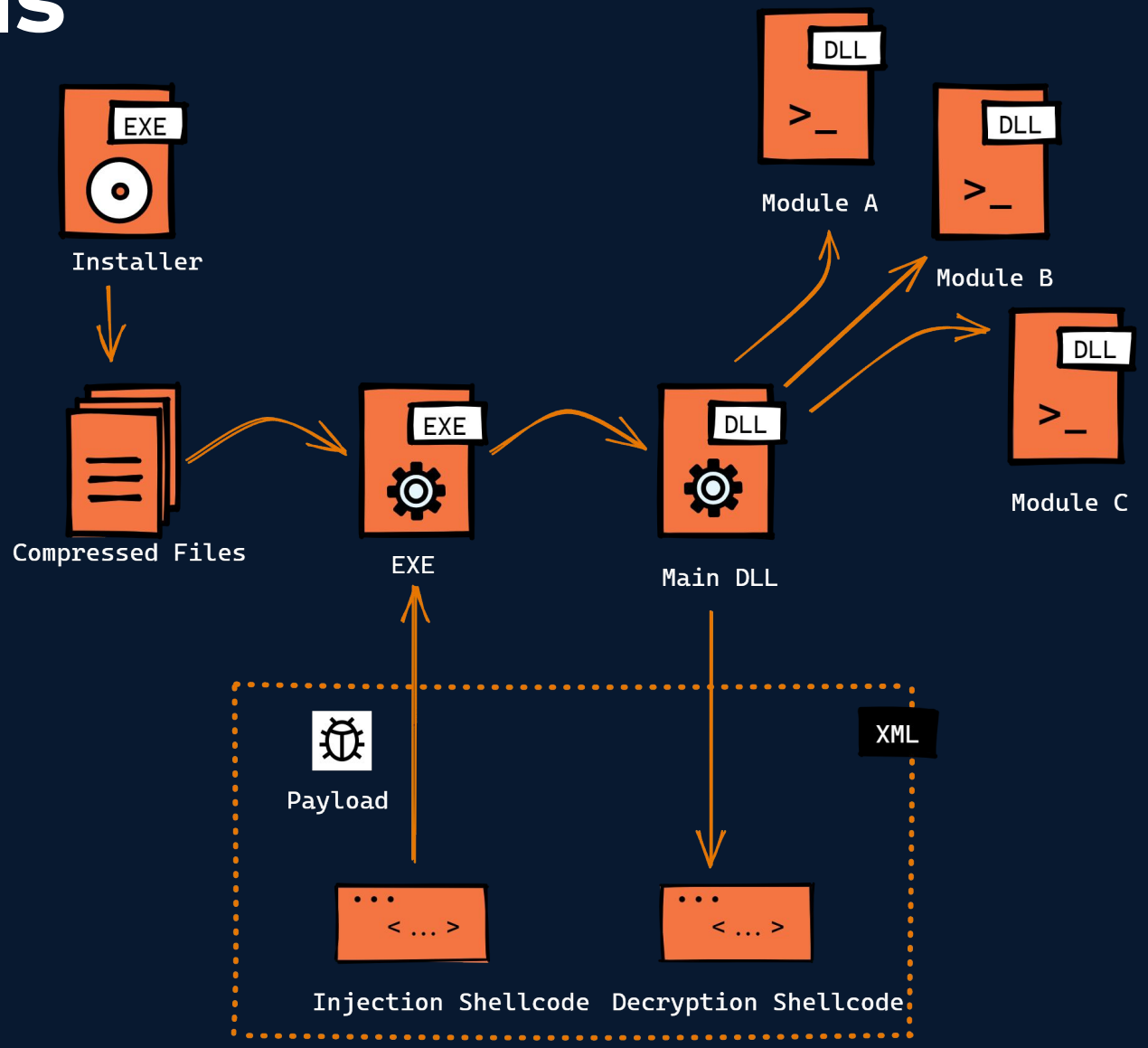
VirusTotal


0
/ 65
Community Score
4c88894f
setup.exe
checks-cp
Previous Analyses
Date order
2021-12-13T14:42:54 UTC 0 / 65
2021-12-15T13:57:29 UTC 0 / 64
2022-01-05T17:48:47 UTC 0 / 65
2022-01-20T08:53:58 UTC 0 / 62
2022-02-18T08:09:42 UTC 0 / 64
2022-02-18T09:26:14 UTC 0 / 66
2022-02-18T10:11:13 UTC 1 / 65
2022-02-18T10:11:43 UTC 1 / 66
2022-02-18T11:05:29 UTC 1 / 66
2022-02-18T11:19:46 UTC 0 / 66
EXE
runtime-modules

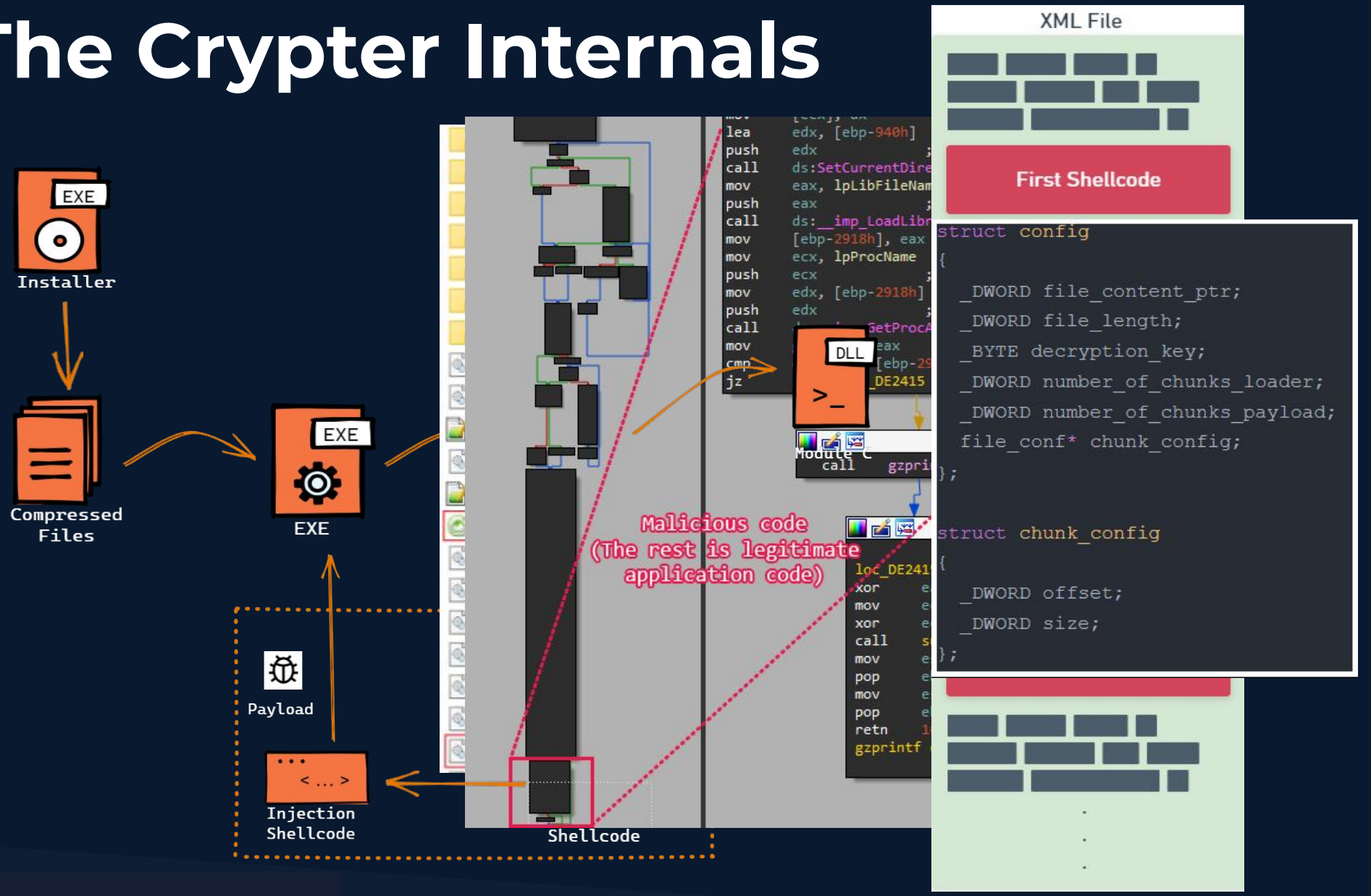

You had my curiosity.

The Crypter Internals

- Crypter Infection chain
  - Installer
  - Executable
  - Main DLL + Modules
  - First stage shellcode
    - “Decryption shellcode”
  - Second stage shellcode
    - “Injection shellcode”



The Crypter Internals



Why BABADEDA ?

```
payload_pe_address = (IMAGE_DOS_HEADER *)0xBABADEDA;
payload_pe_size = 0xDEADBEAF;
payload_optional_header = get_image_optional_header((IMAGE_DOS_HEADER *)0xBABADEDA);
get_nt_header((IMAGE_DOS_HEADER *)0xBABADEDA);
get_image_section_header((IMAGE_DOS_HEADER *)0xBABADEDA);
new_size_of_image = payload_optional_header->SizeOfImage;
current_exe_peb = get_ntcurrpeb();
get_ntcurrteb();
current_exe_address = (IMAGE_DOS_HEADER *)current_exe_peb->ImageBaseAddress;
current_exe_ldr_entry = (LDR_DATA_TABLE_ENTRY *)get_current_exe_ldr_list_entry(current_exe_peb);
new_pe_target_entry_point = (char *)current_exe_address + optional_header->AddressOfEntryPoint;
VirtualProtect = (void (__stdcall *)(IMAGE_DOS_HEADER *, DWORD, MACRO_PAGE, int *))get_func_by_hash_w(new_pe_target_entry_point);
```

- 0xDEADBEAF - Used as a magic debug value
- 0xBABADEDA - In Russian is: Grandma, Grandpa

What makes it so evasive?

- Code logic splitted into several different DLLs
- The code resides in bunch of legitimate application code.
- In newer variants the main DLL is loaded using DLL side-loading technique.
- Encrypted payload and shellcode.

WHAT SHOULD WE DO NEXT?

Analysis

BABADEDA Crypter

WannaCry

TrickBot

Emotet

Qakbot

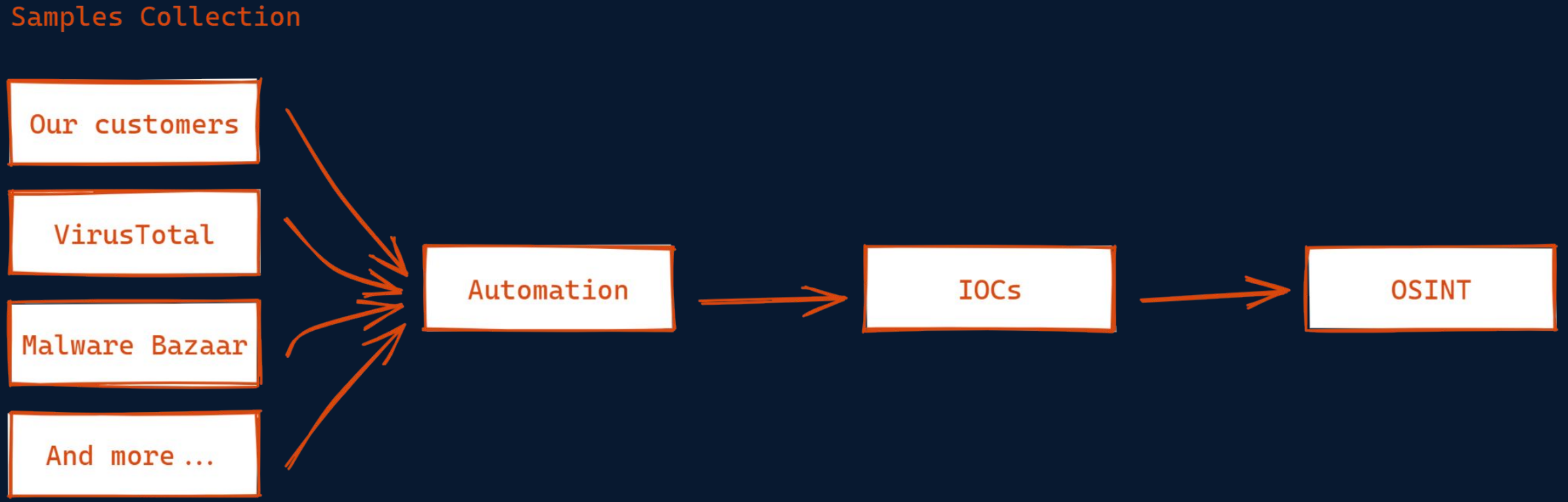
Research

Collecting More Samples

- Translate your knowledge to YARA Rule
- Use your own telemetry as well as open source resources

```
rule BABADEDA_Crypter
{
    meta:
        description = "Detects BABADEDA Crypter"
        author = "Morphisec labs"
        reference = "https://blog.morphisec.com/
        the-babadeda-crypter-targeting-crypto-nft--defi-communities"
    strings:
        $placeholder_1 = {8138DADEBABA}
        $placeholder_2 = {8138AFBEADDE}
        $entry_shellcode = {55 8B EC 83 EC 58 53 E8 F8 03 00 00 89 45 FC 8B 45 FC
        83 C0 11 89 45 CC 8B 45 FC 8B 40 09 8B 4D CC 8D 04}
    condition:
        $entry_shellcode and all of ($placeholder_*)
}
```

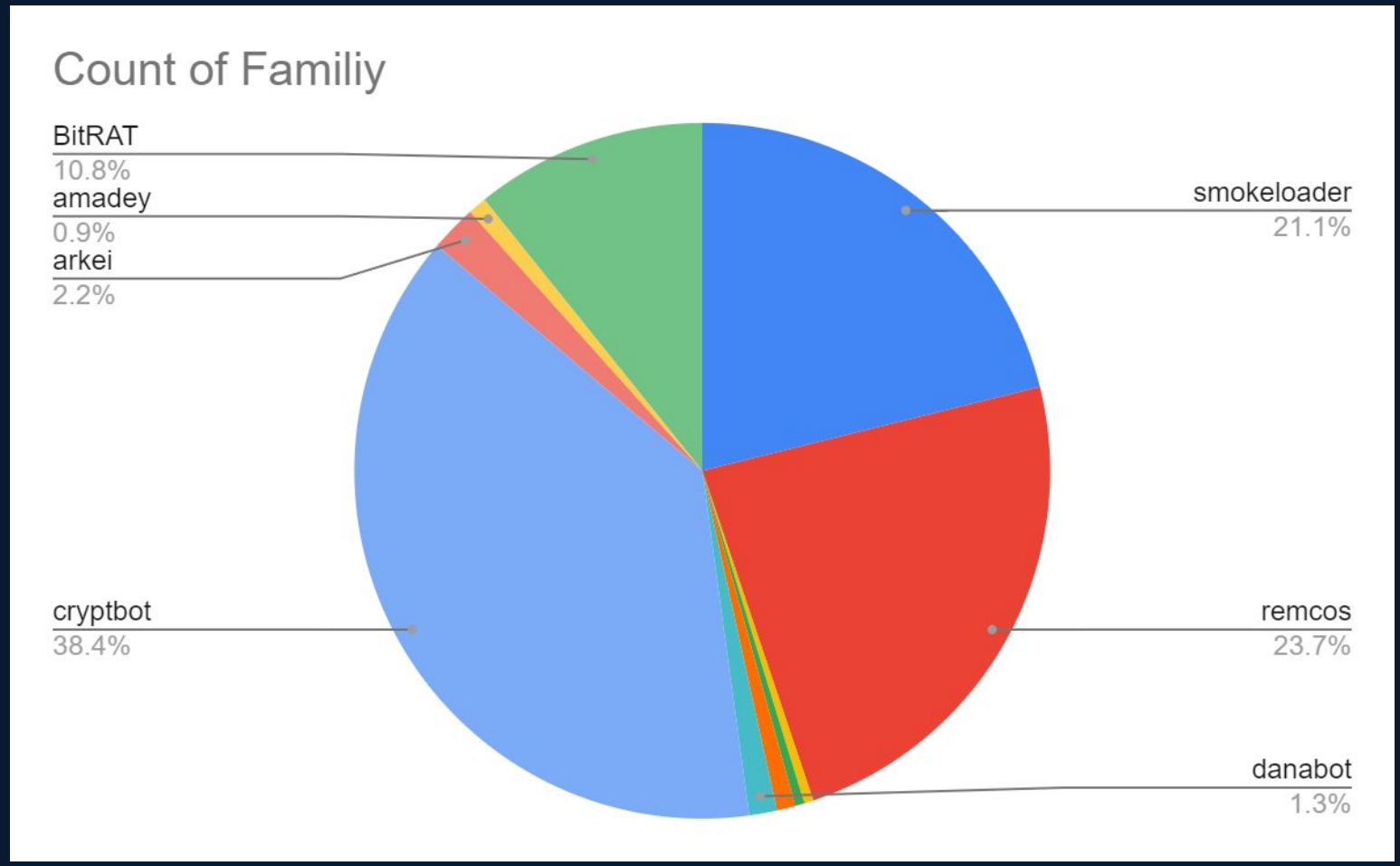
Pipeline Overview

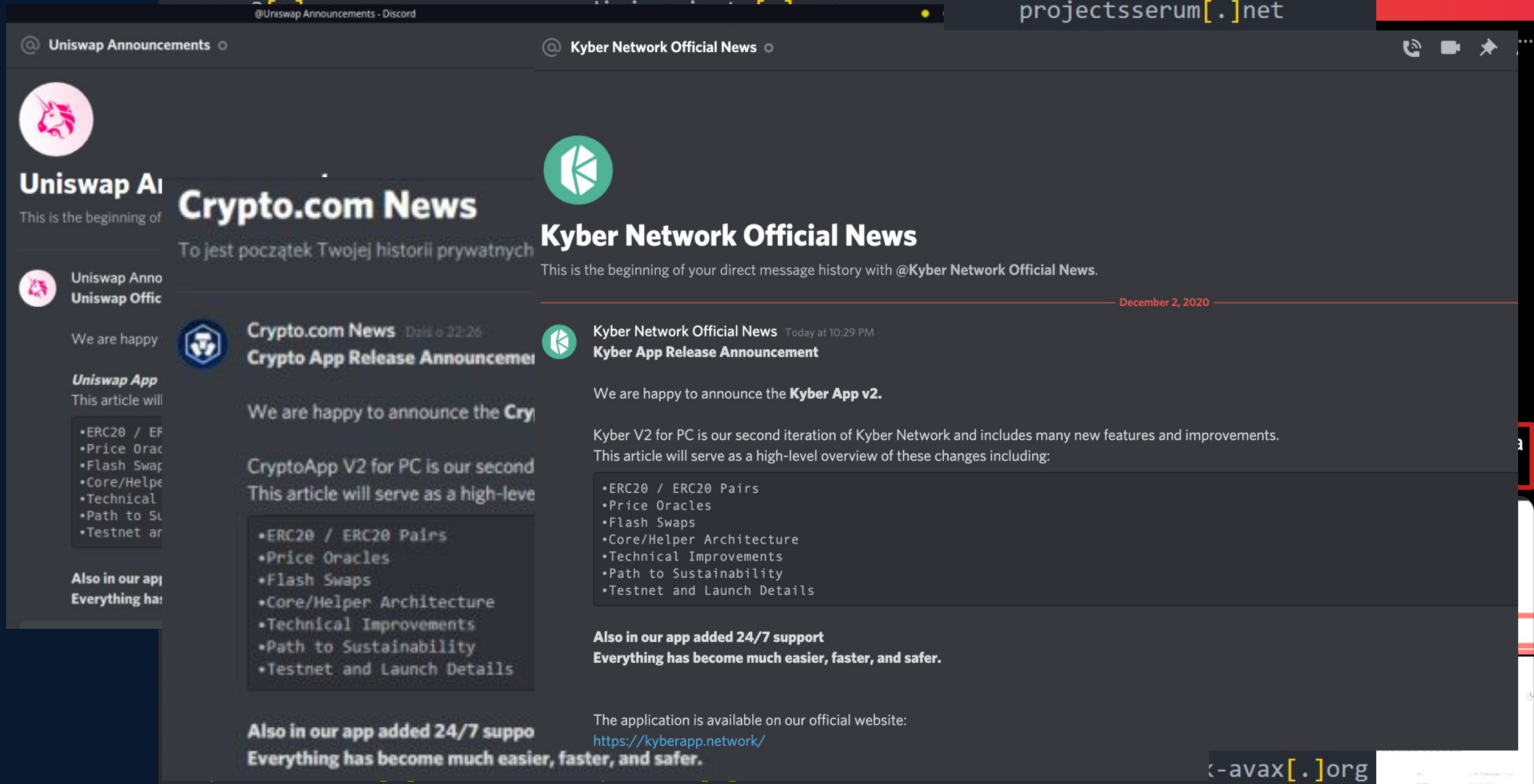


What we are looking for?

- Sample source
- Network activity
- Final payload classification

smokeloader	https://savixtothenation.co.ug/index.php
smokeloader	http://savixtothenation.co.ug/index.php
remcos	193.56.29.242:4783
metasploit	
gozi_ifsb	
fickerstealer	prunerflowershop.com:80
fickerstealer	prunerflowershop.com:80
danabot	192.119.110.73:443
danabot	192.236.147.159:443
danabot	192.210.222.88:443
cryptbot	veowvf15.top
cryptbot	morysl01.top




@Uniswap Announcements - Discord
Uniswap Announcements
Uniswap Ar
This is the beginning of
Uniswap Anno
Uniswap Offic
We are happy
Uniswap App
This article will
•ERC20 / ER
•Price Orac
•Flash Swap
•Core/Helpe
•Technical
•Path to Su
•Testnet ar
Also in our app
Everything has
Crypto.com News
To jest początek Twojej historii prywatnych
Crypto.com News Dziś o 22:26
Crypto App Release Announcemer
We are happy to announce the Cry
CryptoApp V2 for PC is our second
This article will serve as a high-leve
•ERC20 / ERC20 Pairs
•Price Oracles
•Flash Swaps
•Core/Helper Architecture
•Technical Improvements
•Path to Sustainability
•Testnet and Launch Details
Also in our app added 24/7 suppo
Everything has become much easier, faster, and safer.
Kyber Network Official News
Kyber Network Official News
This is the beginning of your direct message history with @Kyber Network Official News.
December 2, 2020
Kyber Network Official News Today at 10:29 PM
Kyber App Release Announcement
We are happy to announce the Kyber App v2.
Kyber V2 for PC is our second iteration of Kyber Network and includes many new features and improvements.
This article will serve as a high-level overview of these changes including:
•ERC20 / ERC20 Pairs
•Price Oracles
•Flash Swaps
•Core/Helper Architecture
•Technical Improvements
•Path to Sustainability
•Testnet and Launch Details
Also in our app added 24/7 support
Everything has become much easier, faster, and safer.
The application is available on our official website:
https://kyberapp.network/
projectsserum[.]net
-avax[.]org
cryptoblade[.]net
decentralands[.]net
polkadot-network[.]com
projectseeds[.]net
wonderlaned[.]com
zed-run[.]net

DeBank Official

Home

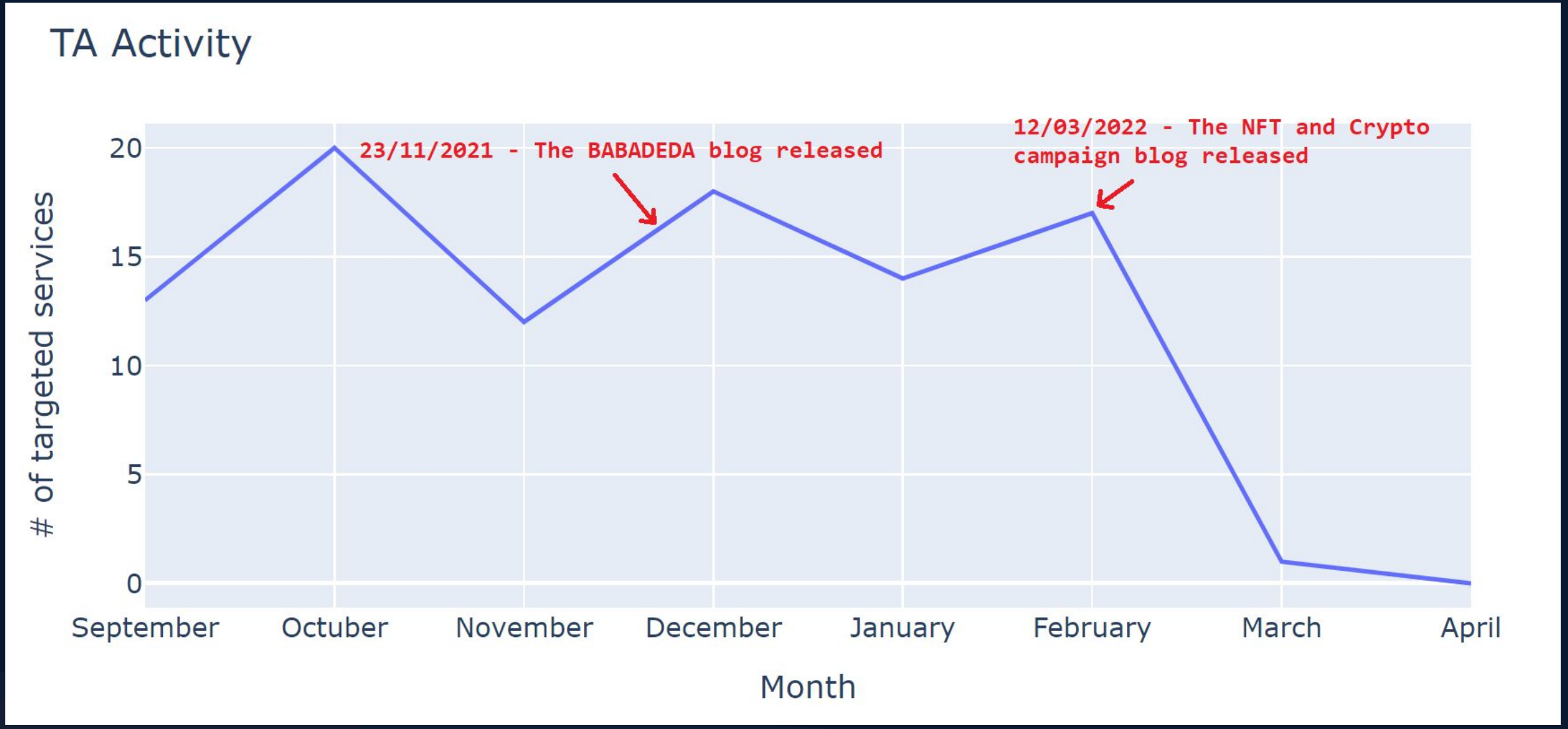
Date	Packer/Crypter	Payload	C2	port
11/2020 - 07/2021	Custom .NET packer	Remcos	95.217.114[.]96 37.48.89[.]8 94.23.218[.]87	4782 4783
07/2021 - 08/2021	Crypto Obfuscator (.NET)	Remcos	135.181.17[.]47	4783
08/2021 - 10/2021	BABADEDA	BitRAT	135.181.140[.]182 135.181.140[.]153 135.181.6[.]215	7777
11/2021 - 12/2021	BABADEDA using DLL sideloading with IIS Express	Remcos AsyncRAT	65.21.127[.]164	4783 4449
12/2021 - *Active	BABADEDA using DLL sideloading with Adobe/TopoEdit	Remcos	193.56.29[.]242	4783
01/2022 - *Active	BABADEDA using DLL sideloading with Link.exe	Remcos	157.90.1.54	4783

DeBank

Best regards, DeBank Project team.

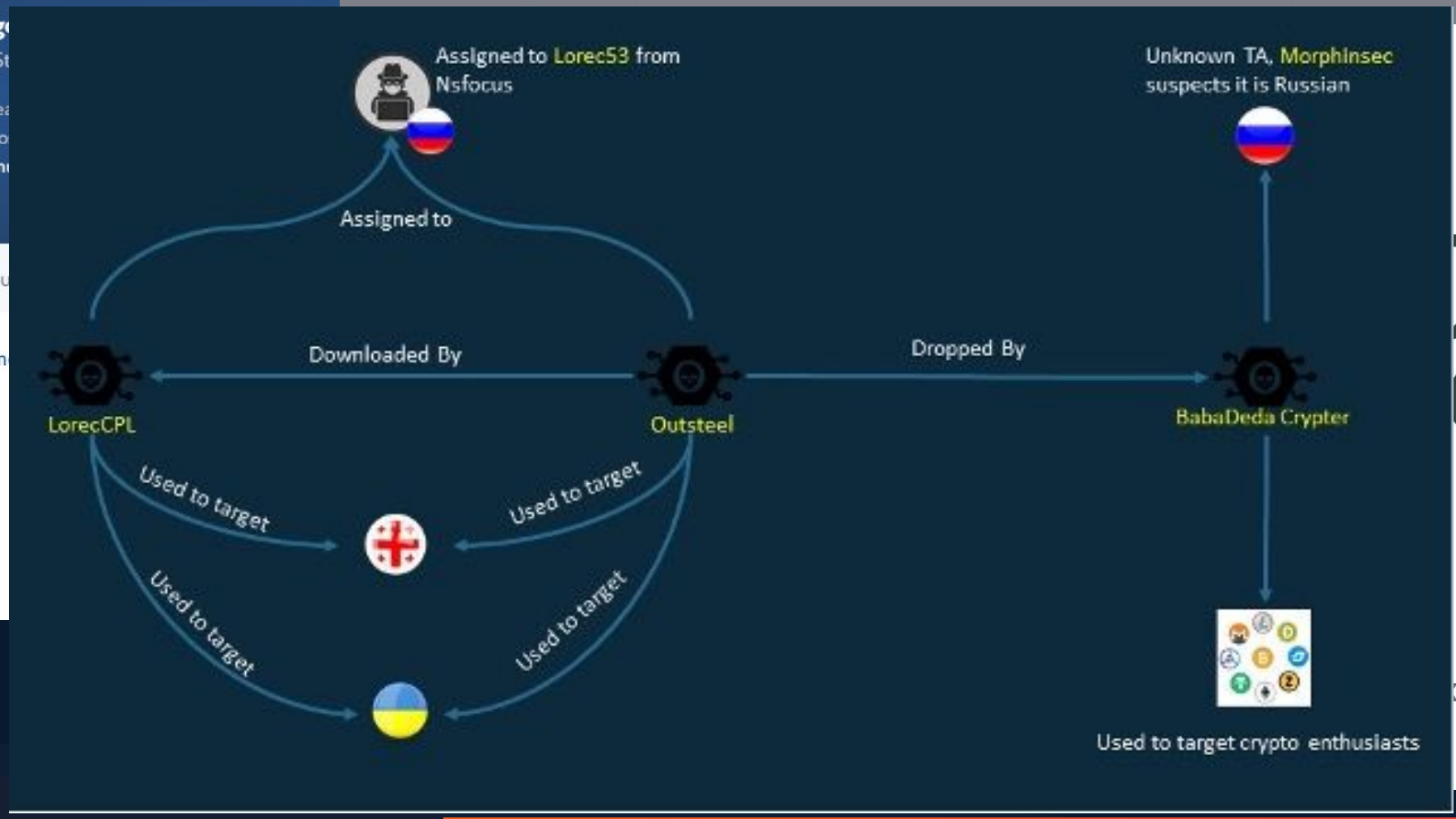
WHY DO WE PUBLISH OUR WORK?

Research Side-effects



BABADEDA Against Ukraine

Telsy



LORECCPL
USED TO
GAINST

KRAINE QUESTION, NEW IOCS, AND

Key takeaways

- Understand the threat landscape your working with
- Look at the bigger picture
- Understand what steps are required to achieve each goal
- Use automations to make your analysis easier
- Share your findings and make use of others researches

Thank You

MORPHISEC

Breach Prevention Made Easy

info@morphisec.com . www.morphisec.com