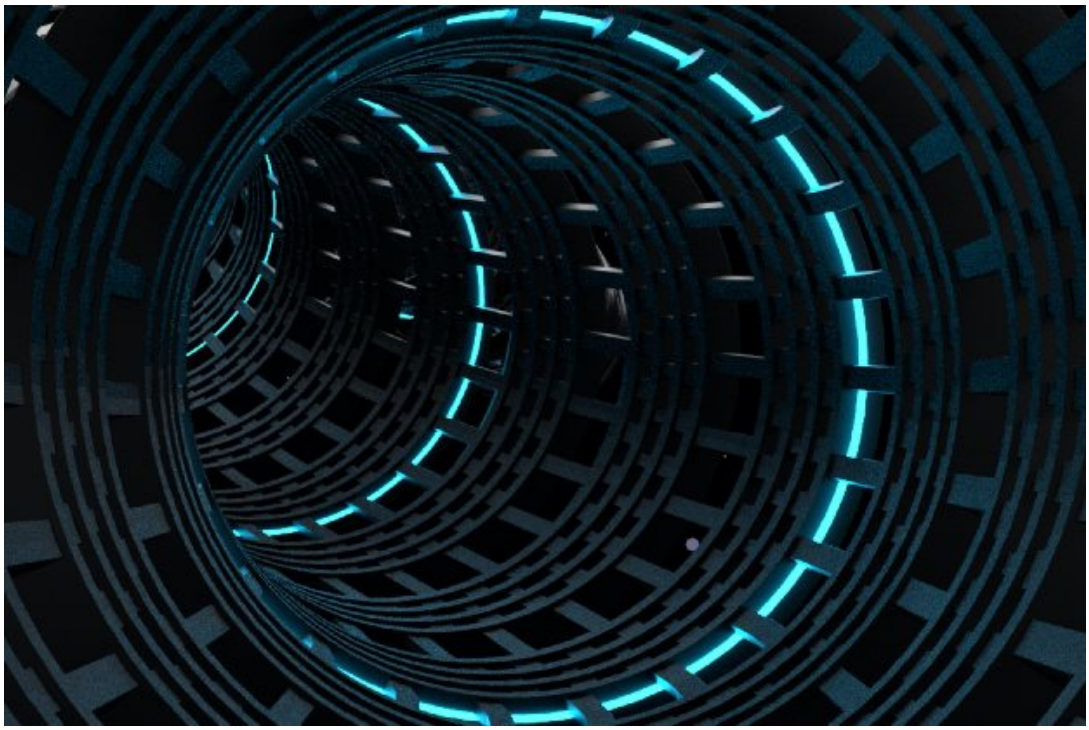
XDSpy: Stealing government secrets since 2011

welivesecurity.com/2020/10/02/xdspy-stealing-government-secrets-since-2011/

October 2, 2020



ESET researchers uncover a new APT group that has been stealing sensitive documents from several governments in Eastern Europe and the Balkans since 2011

Matthieu Faou
2 Oct 2020 - 11:30AM

ESET researchers uncover a new APT group that has been stealing sensitive documents from several governments in Eastern Europe and the Balkans since 2011

Rare is the APT group that goes largely undetected for nine years, but XDSpy is just that; a previously undocumented espionage group that has been active since 2011. It has attracted very little public attention, with the exception of an advisory from the Belarusian CERT in February 2020. In the interim, the group has compromised many government agencies and private companies in Eastern Europe and the Balkans.

This blogpost is a summary, with updated information about the compromise vectors and Indicators of Compromise, of research that we've presented at the Virus Bulletin 2020 conference (see the full paper and the presentation).

Targets

Targets of the XDSpy group are located in Eastern Europe and the Balkans and are primarily government entities, including militaries and Ministries of Foreign Affairs, and private companies. Figure 1 shows the location of known victims according to ESET telemetry.

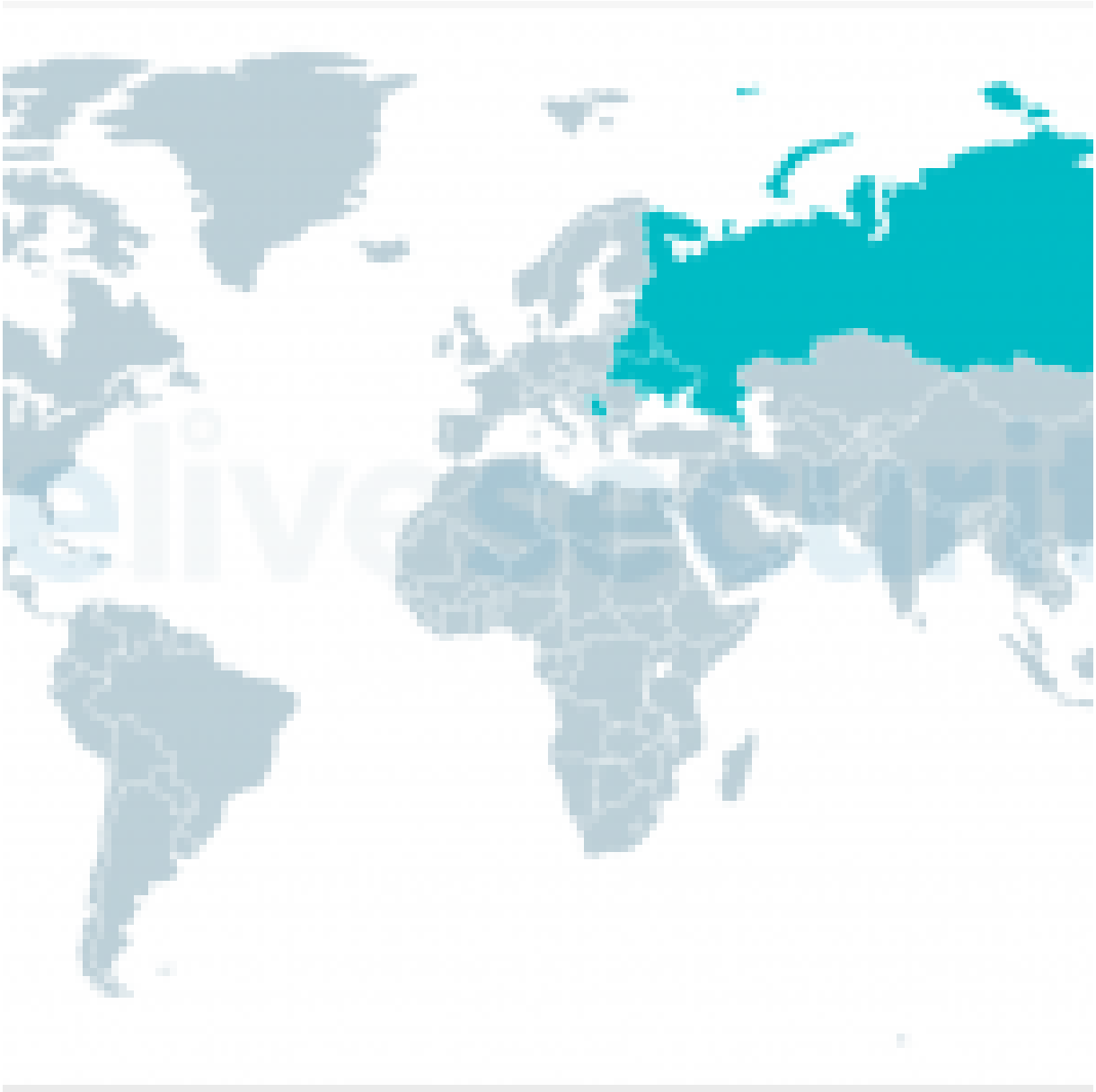


Figure 1. Map of XDSpy victims according to ESET telemetry (Belarus, Moldova, Russia, Serbia and Ukraine)

Attribution

After careful research, we were not able to link XDSpy to any publicly known APT group:

- We did not find any code similarity with other malware families.
- We did not observe any overlap in the network infrastructure.

- We are not aware of another APT group targeting these specific countries and verticals.

Moreover, the group has been active for more than nine years. So, had such an overlap existed, we believe that it would have been noticed, and the group uncovered, a long time ago.

We believe that the developers might be working in the UTC+2 or UTC+3 time zone, which is also the time zone of most of the targets. We also noticed they were only working from Monday to Friday, suggesting a professional activity.

Compromise vectors

XDSpy operators mainly seem to use spearphishing emails in order to compromise their targets. In fact, this is the only compromise vector that we have observed. However, the emails tend to vary a bit: some contain an attachment while others contain a link to a malicious file. The first layer of the malicious file or attachment is generally a ZIP or RAR archive.

Figure 2 is an example of an XDSpy spearphishing email sent in February 2020.

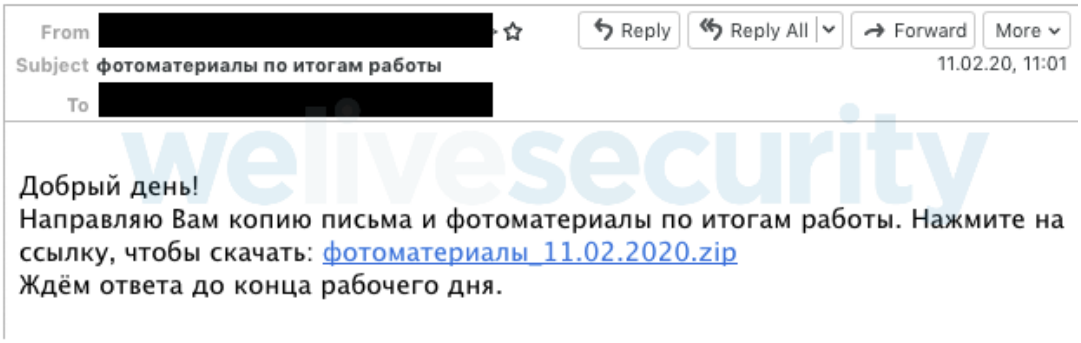


Figure 2. Spearphishing email sent by XDSpy's operators in February 2020

Roughly translated, the body of the email says:

Good afternoon!
I am sending you a copy of the letter and photo materials based on the results of the work. Click on the link to download: photo materials_11.02.2020.zip
We are waiting for an answer until the end of the working day.

The link points to a ZIP archive that contains an LNK file, without any decoy document. When the victim double-clicks on it, the LNK downloads an additional script that installs XDDown, the main malware component.

After our paper was submitted to Virus Bulletin, we continued to track the group and, after a pause between March and June 2020, they came back. At the end of June 2020, the operators stepped up their game by using a vulnerability in Internet Explorer, CVE-2020-0968, which had been patched in April 2020. Instead of delivering an archive with a LNK file, the C&C server was delivering an RTF file that, once opened, downloaded an HTML file exploiting the aforementioned vulnerability.

CVE-2020-0968 is part of a set of similar vulnerabilities in the IE legacy JavaScript engine disclosed in the last two years. At the time it was exploited by XDSpy, no proof-of-concept and very little information about this specific vulnerability was available online. We think that XDSpy either bought this exploit from a broker or developed a 1-day exploit themselves by looking at previous exploits for inspiration.

It is interesting to note that this exploit bears similarities with exploits previously used in DarkHotel campaigns, as shown in Figure 3. It is also almost identical to the exploit used in Operation Domino in September 2020, which was uploaded to VirusTotal from Belarus.

Given that we don't believe XDSpy is linked to DarkHotel and that Operation Domino looks quite different from XDSpy, it is likely that the three groups share the same exploit broker.

Figure 3. Parts of the exploit code, including the beginning, are similar to that used in a DarkHotel campaign described by JPCERT

Finally, the group jumped on the COVID-19 wagon at least twice in 2020. It first used this theme in a spearphishing campaign against Belarusian institutions in February 2020. Then, in September 2020, they reused this theme against Russian-speaking targets. The archive contained a malicious Windows Script File (WSF) that downloads XDDown, as shown in Figure 4, and they used official website rospotrebnadzor.ru as a decoy, as shown in Figure 5.

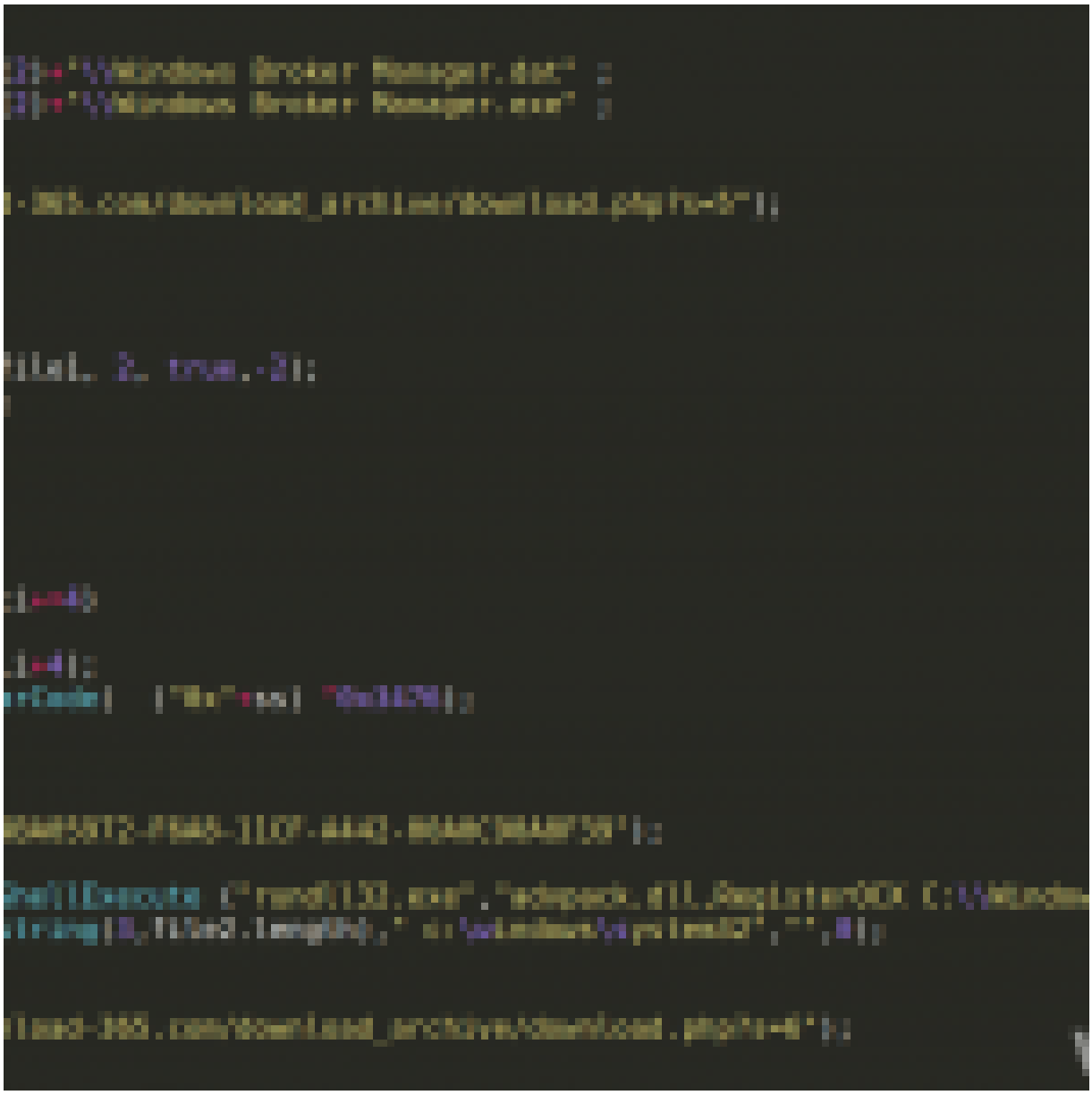


Figure 4. Part of the script that downloads XDDown

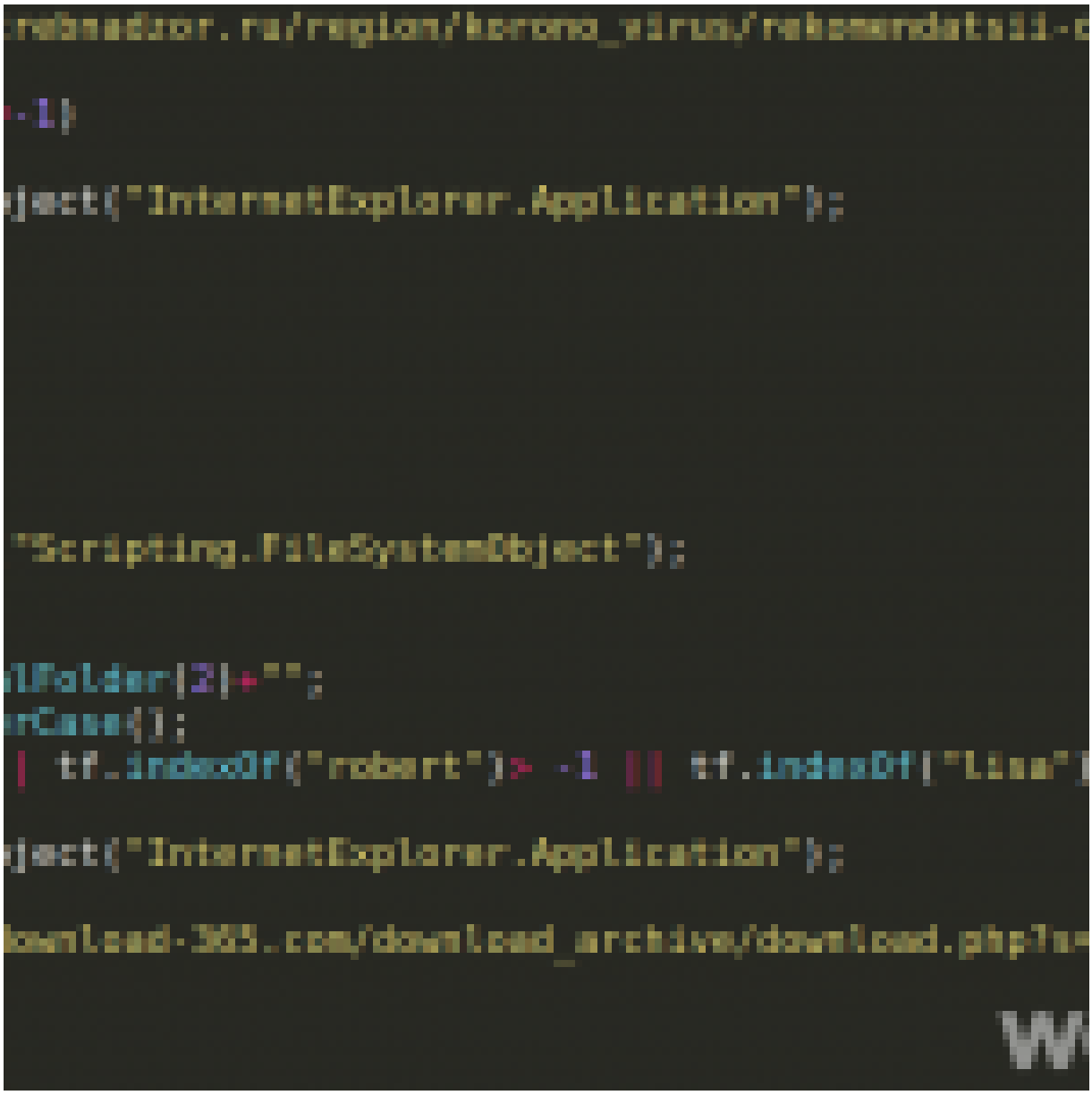


Figure 5. Part of the script that opens the decoy URL

Malware components

Figure 4 shows the malware architecture in a scenario where the compromise happens through a LNK file, as was the case in February 2020.

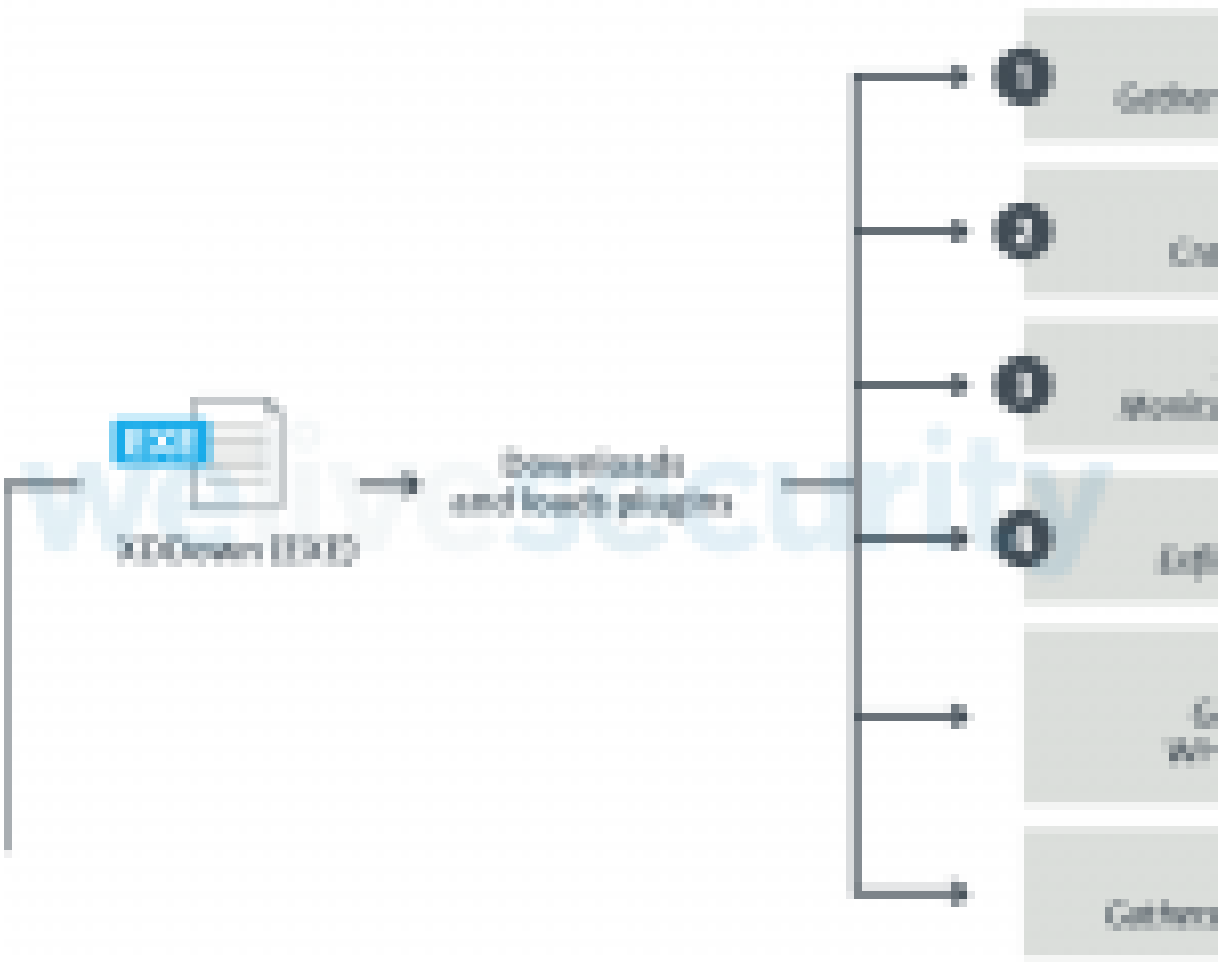


Figure 6. XDSpy's malware architecture. XDLoc and XDPass are dropped in no particular order

XDDown is the main malware component and is strictly a downloader. It persists on the system using the traditional Run key. It downloads additional plugins from the hardcoded C&C server using the HTTP protocol. The HTTP replies contain PE binaries encrypted with a hardcoded two-byte XOR key.

During our research, we discovered the following plugins:

- XDRecon: Gathers basic information about the victim machine (the computer name, the current username and the Volume Serial Number of the main drive).
- XDList: Crawls the C: drive for interesting files (.accdb, .doc, .docm, .docx, .mdb, .xls, .xlm, .xlsx, .xlsm, .odt, .ost, .ppt, .pptm, .ppsm, .pptx, .sldm, .pst, .msg, .pdf, .eml, .wab) and exfiltrates the paths of these files. It can also take screenshots.
- XDMonitor: Similar to XDList. It also monitors removable drives to exfiltrate the files matching an interesting extension.
- XDUpload: Exfiltrates a hardcoded list of files from the filesystem to the C&C server, as shown in Figure 5. The paths were sent to the C&C servers by XDList and XDMonitor.

Figure 7. Loop uploading a hardcoded list of files to the C&C server (partially redacted)

- XDLoc: Gathers nearby SSIDs (such as Wi-Fi access points), probably in order to geo-locate the victim machines.
- XDPass: Grabs saved passwords from various applications such as web browsers and email programs.

More details about the various malware components can be found in the white paper.

Conclusion

XDSpy is a cyberespionage group mostly undetected for more than nine years while being very busy over the past few months. It is mostly interested in stealing documents from government entities in Eastern Europe and the Balkans. This targeting is quite unusual and makes it an interesting group to follow.

The group's technical proficiency tends to vary a bit. It has used the same basic malware architecture for nine years, but it also recently exploited a vulnerability patched by the vendor but for which no public proof-of-concept exists, a so-called 1-day exploit.

For any inquiries, or to make sample submissions related to the subject, contact us at threatintel@eset.com.

Special thanks to Francis Labelle for his work on this investigation.

Indicators of Compromise

The comprehensive list of Indicators of Compromise (IoCs) and samples can be found in our GitHub repository.

Malware components

SHA-1	ESET detection name	Description
C125A05CC87EA45BB5D5D07D62946DAEE1160F73	JS/TrojanDropper.Agent.OAZ	Spearphishing email (2015)
99729AC323FC8A812FA2C8BE9AE82DF0F9B502CA	LNK/TrojanDownloader.Agent.YJ	Malicious LNK downloader
63B988D0869C6A099C7A57AAFEA612A90E30C10F	Win64/Agent.VB	XDDown
BB7A10F816D6FFFECB297D0BAE3BC2C0F2F2FFC6	Win32/Agent.ABQB	XDDown (oldest known sample)
844A3854F67F4F524992BCD90F8752404DF1DA11	Win64/Spy.Agent.CC	XDRecon
B333043B47ABE49156195CC66C97B9F488E83442	Win64/Spy.Agent.CC	XDUpload
83EF84052AD9E7954ECE216A1479ABA9D403C36D	Win64/Spy.Agent.CC	XDUpload
88410D6EB663FBA2FD2826083A3999C3D3BD07C9	Win32/Agent.ABYL	XDLoc
CFD43C7A993EC2F203B17A9E6B8B392E9A296243	Win32/PSW.Agent.OJS	XDPass
3B8445AA70D01DEA553A7B198A767798F52BB68A	DOC/Abnormal.V	Malicious RTF file that downloads the CVE-2020-0968 exploit
AE34BEDBD39DA813E094E974A9E181A686D66069	Win64/Agent.ACG	XDDown
5FE5EE492DE157AA745F3DE7AE8AA095E0AFB994	VBS/TrojanDropper.Agent.OLJ	Malicious script (Sep 2020)
B807756E9CD7D131BD42C2F681878C7855063FE2	Win64/Agent.AEJ	XDDown (most recent as of writing)

Filenames / Paths

%APPDATA%\Temp.NET\archset.dat
%APPDATA%\Temp.NET\hdir.dat
%APPDATA%\Temp.NET\list.dat
%TEMP%\tmp%YEAR%%MONTH%%DAY%_%TICK_COUNT%.s
%TEMP%\fl637136486220077590.data
wgl.dat
Windows Broker Manager.dat
%TEMP%\Usermode COM Manager.dat
%TEMP%\Usermode COM Manager.exe
%APPDATA%\WINinit\WINlogon.exe
%APPDATA%\msprotectexp\mswinexp.exe
%APPDATA%\msvdemo\msbrowsmc.exe
%APPDATA%\Explorer\msdmcm6.exe
%APPDATA%\Explorer\browsms.exe

Network

Used in 2019-2020

downloadsprimary[.]com
filedownload[.]email
file-download[.]org
minisnowhair[.]com
download-365[.]com
365downloading.com
officeupdtcentr[.]com
dropsklad[.]com
getthatupdate[.]com
boborux[.]com
easytosay[.]org
daftsync[.]com
documentsklad[.]com
wildboarcontest[.]com
nomatterwhat[.]info
maiwegwurst[.]com
migration-info[.]com
jerseygameengine[.]com
seatwowave[.]com
cracratutu[.]com
chtcc[.]net
ferrariframework[.]com

Old network infrastructure

62.213.213[.]170
93.63.198[.]40
95.215.60[.]53
forgeron[.]tk
jahre999[.]tk
omgtech.000space[.]com

podzim[.]tk
porfavor876[.]tk
replacerc.000space[.]com
settimana987[.]tk

MITRE ATT&CK techniques

Note: This table was built using version 7 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Initial Access	T1566.001	Phishing: Spearphishing Attachment	XDSpy has sent spearphishing emails with a malicious attachment.
T1566.002	Phishing: Spearphishing Link	XDSpy has sent spearphishing emails with a link to a malicious archive.	
Execution	T1203	Exploitation for Client Execution	XDSpy has exploited a vulnerability (CVE-2020-0968) in Internet Explorer (triggered by a malicious RTF file).
T1204.001	User Execution: Malicious Link	XDSpy has lured targets to download malicious archives containing malicious files such as LNK.	
T1204.002	User Execution: Malicious File	XDSpy has lured targets to execute malicious files such as LNK or RTF.	
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	XDDownload persists using the Run key.
Discovery	T1033	System Owner/User Discovery	XDRecon sends the username to the C&C server.
T1082	System Information Discovery	XDRecon sends the computer name and the main drive Volume Serial Number to the C&C server.	
T1083	File and Directory Discovery	XDList and XDMonitor monitor the local system and the removable drive. A list of interesting paths, that matches a list of hardcoded extension, is sent to the C&C server.	
Collection	T1005	Data from Local System	XDUpload exfiltrates files from the local drive. The paths of the files to be uploaded are hardcoded in the malware samples.
T1025	Data from Removable Media	XDMonitor exfiltrates files from removable drives.	

Tactic	ID	Name	Description
T1113	Screen Capture	XDList, XDMonitor and XDUpload take screenshots and send them to the C&C server.	
T1119	Automated Collection	XDMonitor exfiltrates files from removable drives that match specific extensions. XDUpload exfiltrates local files that are located at one the paths hardcoded in the malware samples.	
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	XDSpy uses HTTP for command and control.
T1573.001	Encrypted Channel: Symmetric Cryptography	XDDownload downloads additional components encrypted with a 2-byte static XOR key.	
Exfiltration	T1020	Automated Exfiltration	XDMonitor and XDUpload automatically exfiltrate collected files.
T1041	Exfiltration Over C2 Channel	XDSpy exfiltrate stolen data using the C&C channel.	

2 Oct 2020 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion