THREAT ALERT: DJvu Variant Delivered by Loader Masquerading as Freeware

Cybereason issues Threat Alerts to inform customers of emerging threats, including a recently observed DJvu variant delivered via a loader masquerading as freeware. Cybereason Threat Alerts summarize these threats and provide practical recommendations for protecting against them.

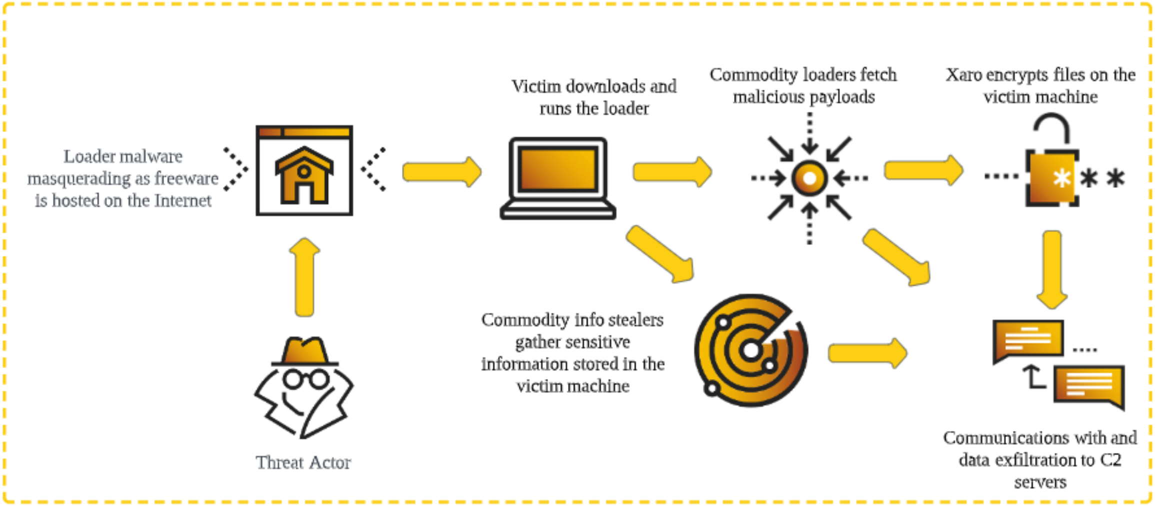
WHAT'S HAPPENING?

The Cybereason GSOC Managed Detection and Response (MDR) Team is investigating incidents that involve variants of the DJvu ransomware delivered via loader payloads masquerading as freeware or cracked software.

While this attack pattern is not new, incidents involving a DJvu variant that appends the .xaro extension to affected files and demanding ransom for a decryptor have been observed infecting systems alongside a host of various commodity loaders and infostealers. This Threat Alert will provide an overview of an attack involving this variant of DJvu, which we will call Xaro for ease of reference.

Impact

The adversary’s goal is data exfiltration, information stealing, and the encryption of files in order to garner a ransom from the victim.


Loader malware masquerading as freeware is hosted on the Internet
Victim downloads and runs the loader
Commodity loaders fetch malicious payloads
Xaro encrypts files on the victim machine
Threat Actor
Commodity info stealers gather sensitive information stored in the victim machine
Communications with and data exfiltration to C2 servers

Attack flow diagram of the Xaro infection- threat actors host malicious payloads as freeware online. When the user downloads and runs the payload, a variety of malware (including the DJvu variant Xaro) is executed.

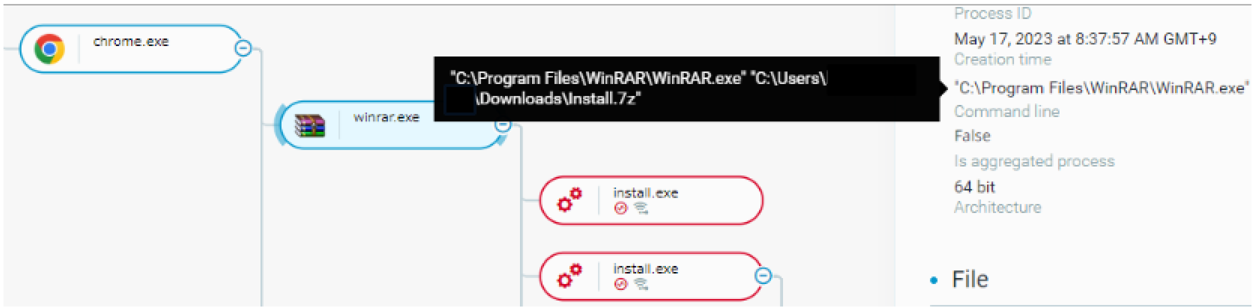
KEY OBSERVATIONS

- **.xaro extension**: The DJvu variant observed in this attack appends the .xaro extension to affected files and drops its ransom note as the file **_readme.txt**. Other DJvu variants appending different extensions to affected files have been observed.
- **Shotgun infection**: Xaro was observed deployed along with a variety of other malicious files, indicating a ‘shotgun’ approach undertaken by the threat actor.
- **The risks of freeware**: This attack illustrates the risks involved with downloading freeware from untrusted sources.

ANALYSIS

Infection Flow

The infection begins with the user downloading the archive file **install.7z** from an untrusted source masquerading as a site that distributes legitimate freeware. The archive is opened via an unarchiving tool such as Winrar and the file **install.exe** is run.

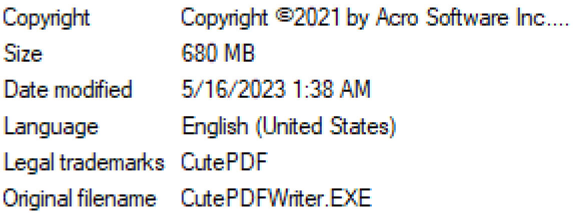


"C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\[redacted]\Downloads\Install.7z"

Process ID
May 17, 2023 at 8:37:57 AM GMT+9
Creation time
"C:\Program Files\WinRAR\WinRAR.exe"
Command line
False
Is aggregated process
64 bit
Architecture

Initial infection vector

The Install.exe file itself is a fairly large (680MB) packed binary file. An analysis of the file's metadata suggests that it is attempting to masquerade as a PDF writing software.



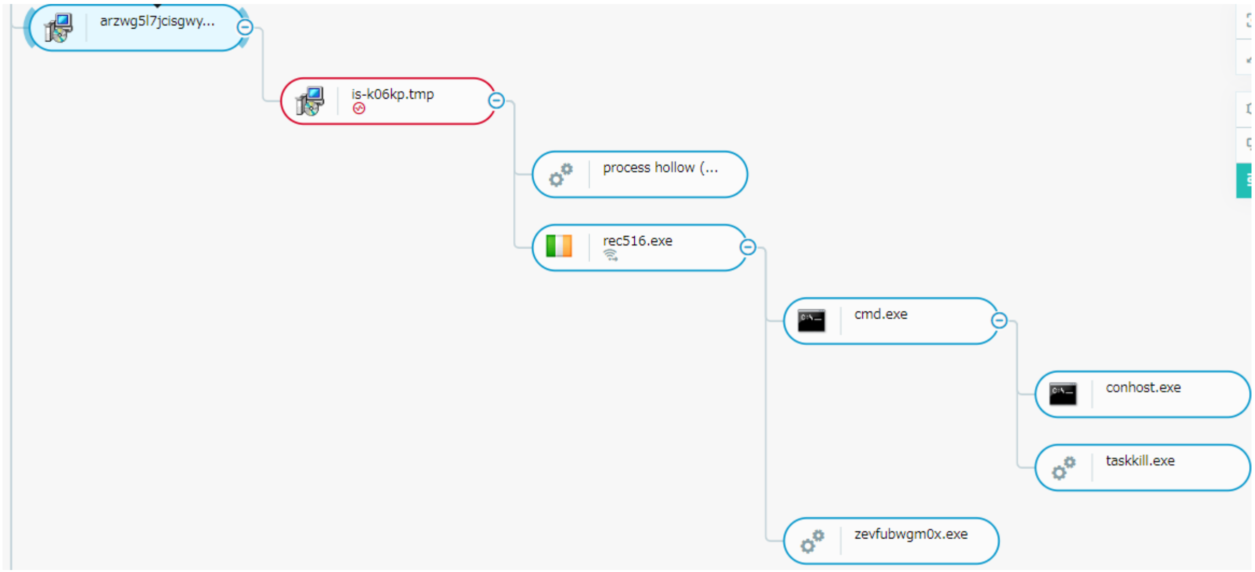
Copyright	Copyright ©2021 by Acro Software Inc....
Size	680 MB
Date modified	5/16/2023 1:38 AM
Language	English (United States)
Legal trademarks	CutePDF
Original filename	CutePDFWriter.EXE

Install.exe metadata

The file hash for install.exe is unknown to public threat intelligence as of this writing, however sandbox analysis suggests that it is an instance of PrivateLoader. PrivateLoader is a pay-per-install modular downloader first observed in 2021 and often observed on sites offering freeware or cracked versions of legitimate software.

Install.exe was observed communicating with C2 servers in the Russian Federation, Malaysia, and Denmark, with the majority of data retrieved from a domain associated with the Russian social media service VK. This communication resulted in the downloading and execution of a variety of commodity malware including:

- Redline Stealer: An infostealer program that can find and exfiltrate sensitive data stored in browsers, cryptocurrency wallets, and third party applications, as well as act as a downloader for other malware.
- Vidar: An infostealer program that focuses primarily on gathering and exfiltrating data, account credentials, cryptocurrency wallet information, and more.
- Amadey: A Russian-based botnet program that can send information about infected machines to C2 servers and act as a loader.
- SmokeLoader: a modular malware loader program primarily used to introduce new malware into an infected system.
- Nymaim: A downloader program sometimes observed with PrivateLoader that displays a lock screen as it downloads further malware.
- GCleaner: A module loader program originally advertised to victims as a desktop optimization tool.
- XmRig: A cryptocurrency miner often found bundled with malware to mine the Monero cryptocurrency.
- Fabookie: An infostealer program specializing in stealing information related to Facebook accounts.
- LummaC Stealer: A Russian-based MaaS platform that operates as an infostealer program.



Redline and Nymaim attack tree

This shotgun-approach to the download and execution of commodity malware is commonly observed in PrivateLoader infections originating from suspicious freeware or cracked software sites and appears to meet four main goals:

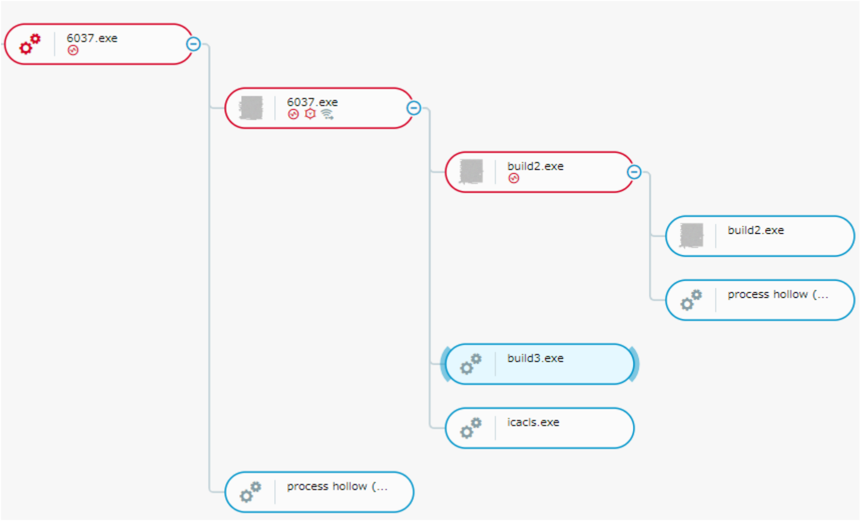
1. Complicate investigation efforts by using multiple loaders to obfuscate the execution of other payloads.
2. Use the various information stealing capabilities of the various payloads to gather and exfiltrate sensitive information even as new payloads are downloaded and executed from C2 servers.
3. Leverage a diversity of tactics to ensure that the infection can succeed as a whole even if one payload is blocked.
4. Create persistence via a large number of registry entries and scheduled tasks.

Xaro

The initial Xaro payload was observed running on the victim machine within **three minutes** of the program install.exe's first execution. The payload is executed and terminated several times, with two distinct execution flows observed. The execution flows differ in their goals but share certain characteristics, such as creating a copy of the malware in the **C:\Users\User\AppData\Local\[Randomly generated UUID]** directory.

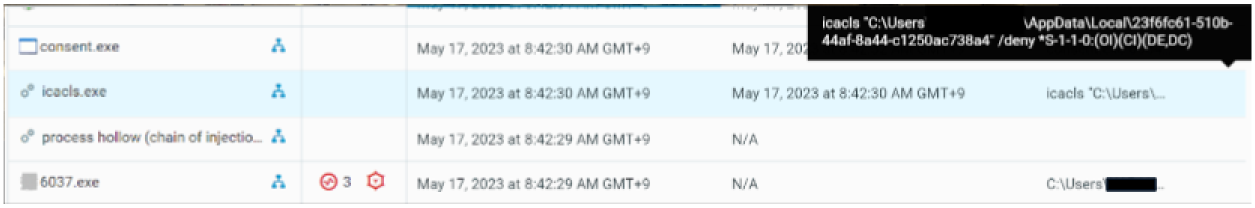
First Flow

The process runs under a randomized name four alphanumeric characters long (for example **5r64.exe**) and spawns a child process of itself into which it injects code via process hollowing before terminating. This child process creates runtime registry keys for persistence at the location **\software\microsoft\windows\currentversion\run\syshelper** and connects to C2 servers, which we have observed to be related to the following domains: **colisumy[.]com**, **zexeq[.]com**, **api.2ip[.]ua**



First flow attack tree

As observed in some other samples related to DJvu the Xaro process utilizes the Windows command line utility process **icalcs.exe** to deny the well-known SID S-1-1-0 (meaning all users in the environment) access objects in its directory with explicit denial of delete commands run either on itself or its children.



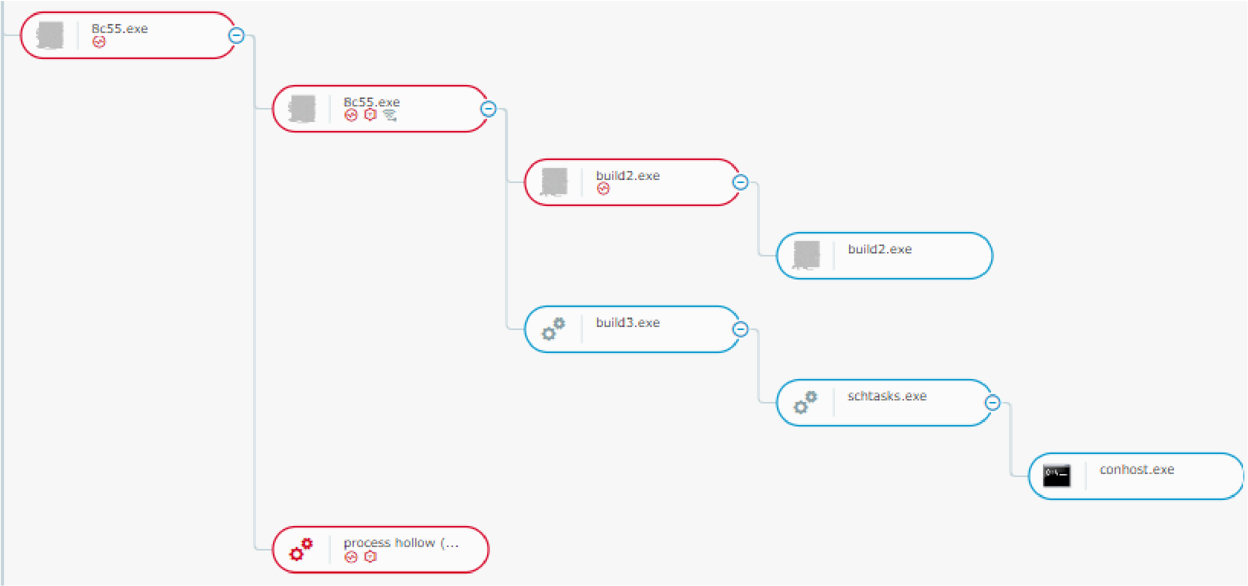
icacls "C:\Users [redacted] \AppData\Local\23f6fc61-510b-44af-8a44-c1250ac738a4" /deny *S-1-1-0:(OI)(CI)(DE,DC)

consent.exe		May 17, 2023 at 8:42:30 AM GMT+9	May 17, 202	
icacls.exe		May 17, 2023 at 8:42:30 AM GMT+9	May 17, 2023 at 8:42:30 AM GMT+9	icacls "C:\Users\...
process hollow (chain of injectio...		May 17, 2023 at 8:42:29 AM GMT+9	N/A	
6037.exe	3	May 17, 2023 at 8:42:29 AM GMT+9	N/A	C:\Users\[redacted]...

icalcs.exe called after the Xaro process

Once done, the Xaro process spawns an instance of the Vidar infostealer and Clipbanker in the protected directory under the names **build2.exe** and **build3.exe**.

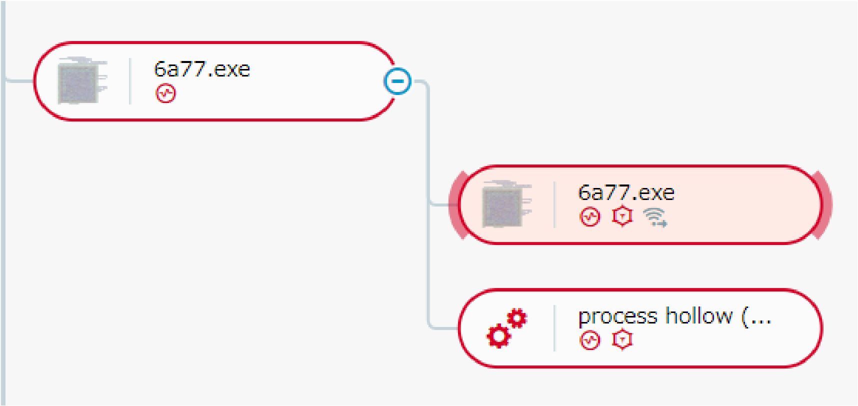
Executions were observed where this activity led to a scheduled task named **Azure-Update-Task** being created to run the **mstsca.exe**, a file often seen dropped with DJvu.



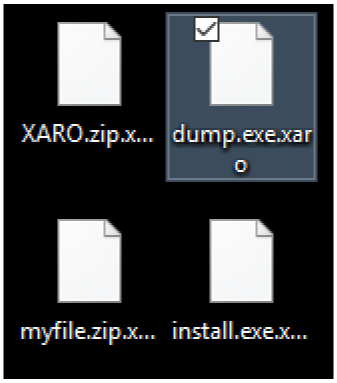
First flow attack tree with scheduled task creation

Second Flow

Roughly **fifteen minutes** after initial infection the second distinct execution occurs, where a new process with a randomly generated four alphanumeric character long name is spawned. As before this process spawns a child of itself into which it performs process hollowing and then terminates, likely in an attempt to complicate investigation and bypass security measures. This child process was observed connecting to the C2 server **api.2ip[.]ua**. Unlike the first flow, this second flow instead begins encrypting files in the **C:\Users\User** directory on the affected machine using the AES-256 algorithm.

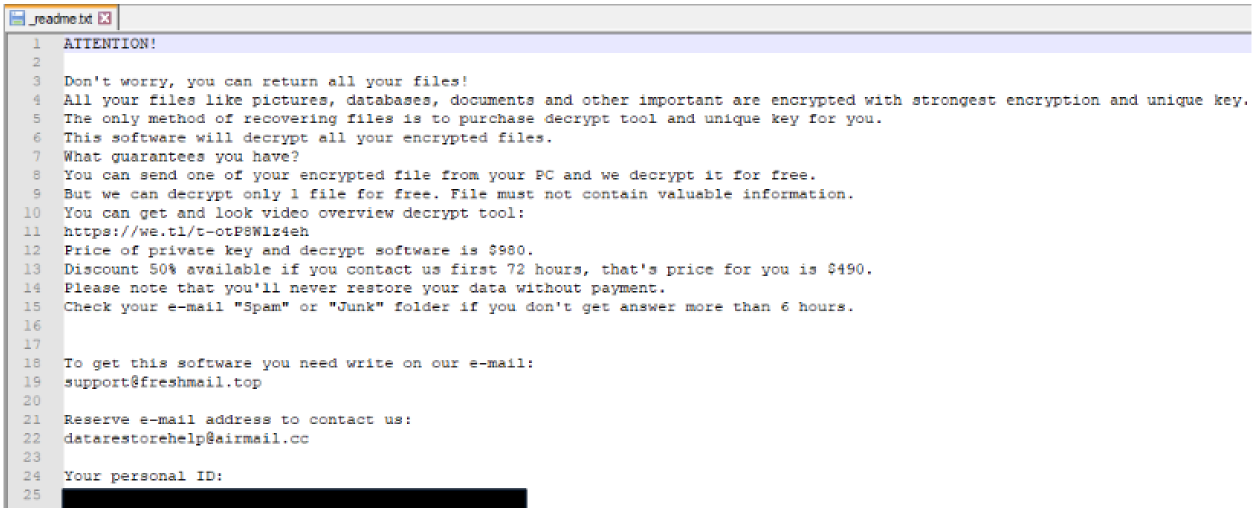


Second flow attack tree



Files encrypted by Xaro

Once the encryption algorithm has finished, Xaro drops its ransom note in the directory **C:\Users\User** as the text file **_readme.txt**



```
ATTENTION!

Don't worry, you can return all your files!
All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
https://we.tl/t-otP8Wlz4eh
Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.


To get this software you need write on our e-mail:
support@freshmail.top

Reserve e-mail address to contact us:
datarestorehelp@airmail.cc

Your personal ID:
[redacted]
```

Xaro ransom note _readme.txt

ATTENTION!

Don't worry, you can return all your files!
All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
https://we.tl/t-otP8WIz4eh
Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.

To get this software you need write on our e-mail:
support@freshmail.top

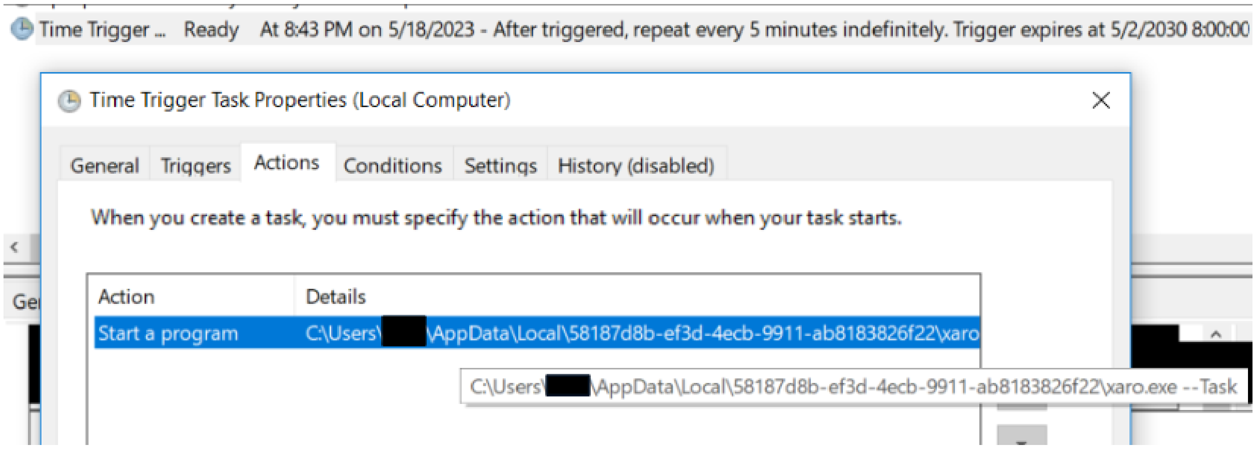
Reserve e-mail address to contact us:
datarestorehelp@airmail.cc

Your personal ID:
[Generated ID]

Copy of ransom note text

As is typical with ransomware, payment is demanded for a decryption tool with discounts offered for quick payment to disincentivize the victim from attempting to investigate further or spend time attempting to decrypt the files themselves.

On top of the previously observed registry entry used for persistence, this execution sets a scheduled task with the task name **Time Trigger Task** that reruns the Xaro payload stored in the C:\Users\User\AppData\Local\[Randomly generated UUID]\ directory, encrypting any new files introduced to the environment.



Time Trigger ... Ready At 8:43 PM on 5/18/2023 - After triggered, repeat every 5 minutes indefinitely. Trigger expires at 5/2/2030 8:00:00

Time Trigger Task Properties (Local Computer)

When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	C:\Users\[redacted]\AppData\Local\58187d8b-ef3d-4ecb-9911-ab8183826f22\xaro

C:\Users\[redacted]\AppData\Local\58187d8b-ef3d-4ecb-9911-ab8183826f22\xaro.exe --Task

Indicators of Compromise

Below is a list of IoCs observed in this attack. Note that certain IoCs may differ across different attacks:

Type	**Value**	**Comment**
SHA-256	10ef30b7c8b32a4c91d6f6fee738e39dc0 2233d71ecf4857bec6e70520d0f5c1	install.exe
SHA-256	83546201db335f52721ed313b9078de267 eaf1c5d58168b99e35b2836bf4f0fc	Xaro payload
SHA-256	3d9cf227ef3c29b9ca22c66359fdd61d9b 3d3f2bb197ec3df42d49ff22b989a4	Build2.exe
SHA-256	8d7f0e6b6877bdfb9f4531afafd0451f7d1 7f0ac24e2f2427e9b4ecc5452b9f0	Build3.exe
Domain	api.2ip[.]ua	Xaro C2 server

Domain	colisumy[.]com	Xaro C2 server
Domain	zexeq[.]com	Xaro C2 server
Task Name	Azure-Update-Task	Scheduled task
Task Name	Time Trigger Task	Scheduled task used to rerun Xaro
Registry	software\microsoft\windows\currentversion\run\syshelper	Registry entry used by Xaro for persistence

These indicators can be used for threat hunting purposes.

Conclusions

While this kind of attack is not novel, the speed and breadth of impact on infected machines should be carefully understood by enterprise networks looking to defend themselves and their data. Within fifteen minutes of infection C2 communications had been established, secondary and tertiary payloads downloaded and executed, sensitive data accessed and exfiltrated, several forms of persistence established, and ransomware run. Faced with this kind of threat, protection at the endpoint is critical.

Threat actors are known to favor freeware masquerading as a way to covertly deploy malicious code. Moreover, while in this case the .xaro extension was added to affected files, DJvu variants that add other extensions have been observed in the wild. Users should be educated about the risks associated with downloading and using software from untrusted sources to mitigate the risk of infection.

CYBEREASON RECOMMENDATIONS

The Cybereason Defense Platform can detect and prevent post-exploitation observed in attacks using DJvu variants. Cybereason recommends the following actions:

- Enable Anti-Ransomware and set it to **Prevent** to ensure maximum protection against ransomware.
- In the Cybereason Defense Platform, enable Application Control to block the execution of malicious files.
- To hunt proactively, use the Investigation screen in the Cybereason Defense Platform and the queries in the Hunting Queries section to search for assets that have potentially been exploited. Based on the search results, take further remediation actions, such as isolating and re-imaging the affected machines.
- Ensure that users are educated on the risks of downloading freeware from untrusted sources or cracked software.
- Add the aforementioned IoCs to your environment's custom reputation list with the "Block & Prevent" flags.

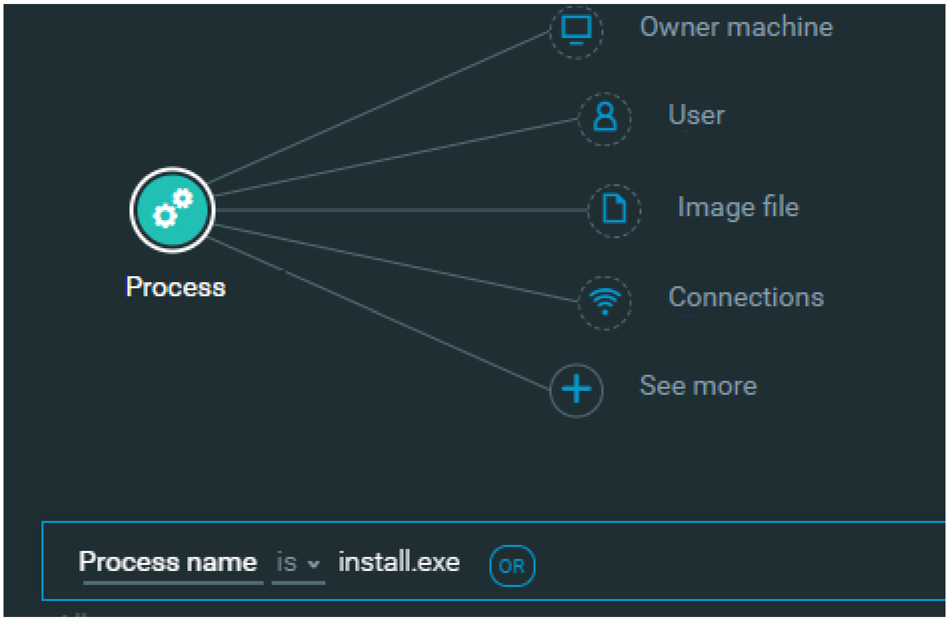
HUNTING QUERIES

We recommend running queries to look for indicators of compromise associated with Xaro. To detect if an attack similar to the above has affected your environment, run the following hunting queries in the Cybereason Defense Platform.

Hunting for install.exe

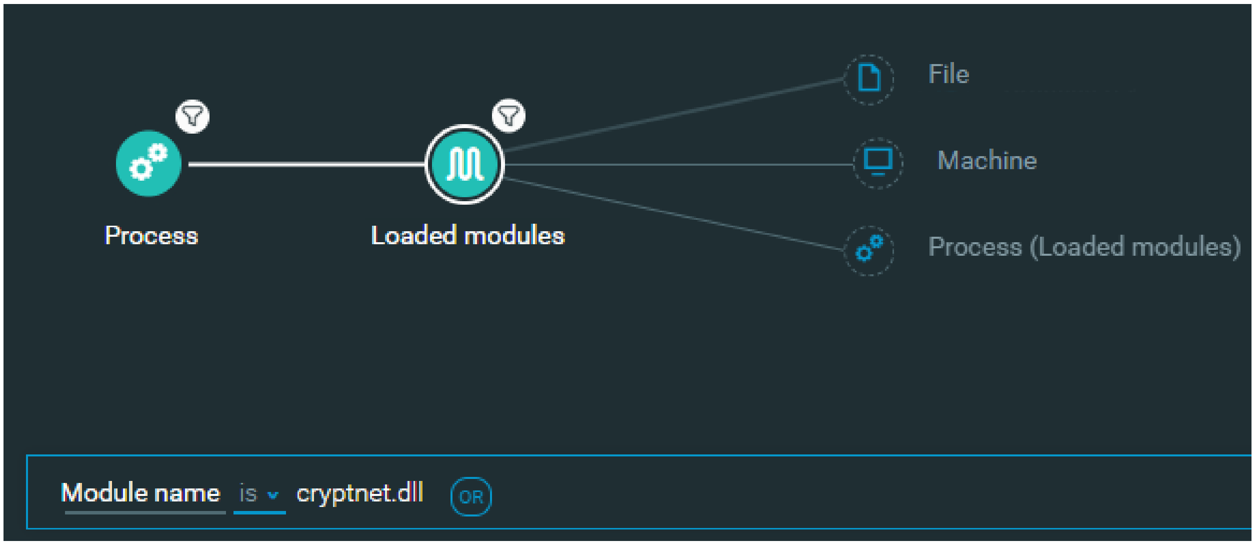
To search for the PrivateLoader sample observed in the attack above, run the following query:

1. **Process** Element -> add the filter **Process name is install.exe**



Process name is install.exe OR

2. **Loaded module** Element -> add the filter **Module name is cryptnet.dll**



Module name is cryptnet.dll OR

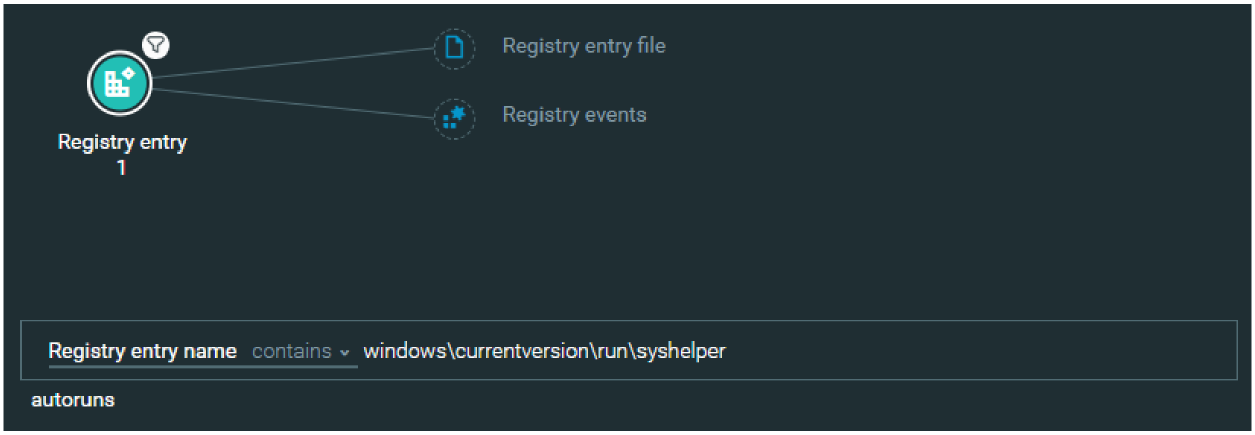
We provided the following hunting query to obtain the same result:

[https://[yourenvironment]](https://[yourenvironment])/#/s/search?queryString=1<-@1684314721120-1684401121120 @Process"elementDisplayName:%3Dinstall.exe"->loadedModules"elementDisplayName:%3Dcryptnet.dll"

Hunting for persistence

To search for the registry entry used by Xaro for persistence, use the following query:

1. **Registry entry** Element -> add the filter **Registry entry name contains \windows\currentversion\run\syshelper**



Registry entry name contains windows\currentversion\run\syshelper

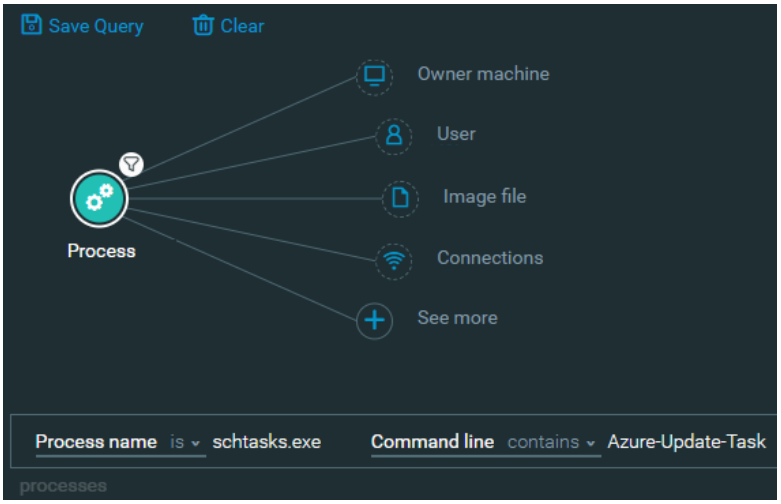
autoruns

We provided the following hunting query to obtain the same result:

[https://[yourenvironment]/#/s/search?queryString=0](https://[yourenvironment]/#/s/search?queryString=0)<-Autorun"elementDisplayName:@windows%5Ccurrentversion%5Crun%5Csyshelper"

To search for the creation of the scheduled task "Azure-Update-Task" used by Xaro for persistence, use the following query:

1. **Process** Element -> add the filters **Process name is 'schtasks.exe'** AND **command line contains 'Azure-Update-Task**'



Process name is schtasks.exe Command line contains Azure-Update-Task

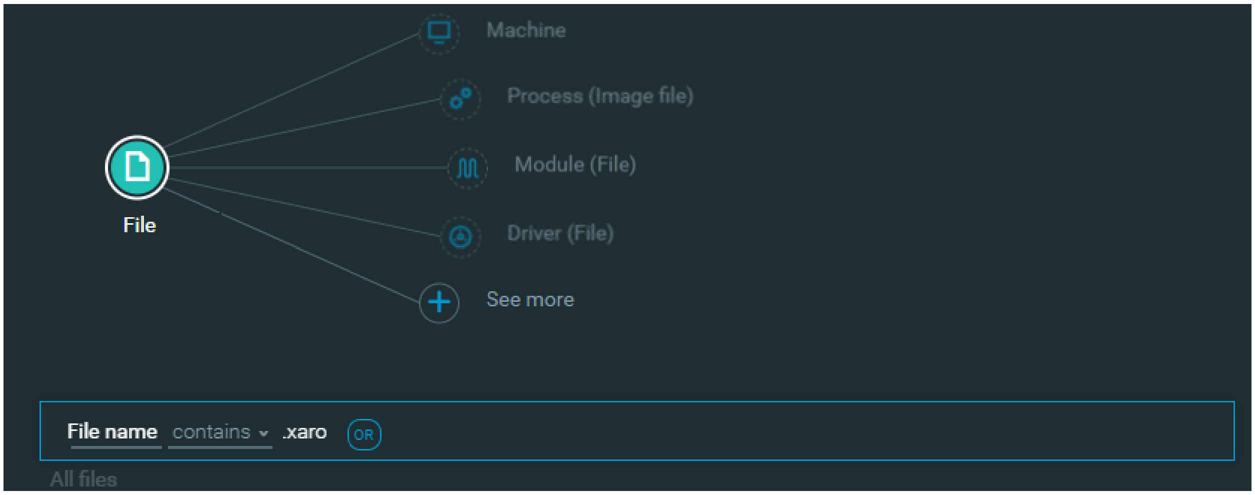
We provided the following hunting query to obtain the same result:

https://[yourenvironment]/#/s/search?queryString=0<-Process"elementDisplayName:%3Dschtasks.exe,commandLine:@Azure-Update-Task"

Hunting for files appended with .xaro

To search for files affected by Xaro, run the following hunting query in the Cybereason Defense Platform:

1. **File** Element -> add the filter **File name matches pattern .xaro**

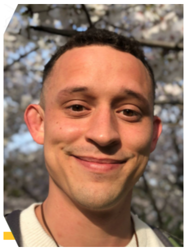


File name contains .xaro

We provided the following hunting query to obtain the same result:

https://[yourenvironment]/#/s/search?queryString=0<-File"elementDisplayName:@.Xaro"

ABOUT THE RESEARCHER



Ralph Villanueva, Senior Security Analyst, Cybereason Global SOC

Ralph Villanueva is a Security Analyst with the Cybereason Global SOC team. He works hunting and combating emerging threats in the cybersecurity space. His interests include malware reverse engineering, digital forensics, and studying APTs. He earned his Masters in Network Security from Florida International University.