Static Analysis

1. Virus Total Analysis

Hash Analysis

- File Hash: [Insert MD5, SHA-1, SHA-256 hash value]
    - MD5:5302477a2c210083be8d25280a1d27cf
    - SHA-1:7d9cfcfe09c52303e9ab741353c06e014364cdd6
    - SHA-256:c40b21462fa3c5ebbed41befc33078f7453e4ed5e2594a815103c1efe70d6327
- Method of hash acquisition: [Describe process]
    - I found the hashes on virustotal
- [Link to VirusTotal results]
    - https://www.virustotal.com/gui/file/c40b21462fa3c5ebbed41befc33078f7453e4ed5e2594a815103c1efe70d6327/details

Vendor Analysis

- Number of vendors flagging as malicious: [X/Y]
    - 57/71
- Analysis of vendor results:
    - [Discuss patterns in detection]
        - Trojan, ransomware, injector, backdoor
    - [Common malware names identified]
        - Loki, PWSX-gen, Infostealer, msil, SnakeStealer, Kryptik
    - [Notable vendor disagreements]
        - Some vendors call this a ransomware, and some call it a trojan. Some call this virus Loki, while others call it MSIL-Kryptik

File History

- First Submission Date: [Date]
- File Creation Date from Windows: [Date]
    - Creation Time: 2022-05-10 01:06:57 UTC
    - First Seen In The Wild: 2025-02-03 17:29:26 UTC
    - First Submission: 2025-02-03 17:18:15 UTC
- Analysis of submission timeline:
    - [Discussion of file age]
        - The file is almost 3 years old
    - [Notable resubmissions or changes]
        - File name has changed
            - TikTokBypassCensor.exe
            - TikTokBypass.exe
            - Week3.exe

Community Score

- [Link to your VirusTotal community contribution]
- Summary of initial findings posted to the community:
    - [Key observations]
    - [Potential indicators of compromise]

2. Detect It Easy (DIE) Analysis

File information

- File type: [Type]
    - PE32
- Architecture: [Architecture]
    - i386
- Compiler: [Compiler information]
    - cli (from Ghidra)
- Additional relevant information:
    - Language: C#
    - Microsoft Linker
    - OS: Windows 95
    - Copyright © 2025 ByteDance Software Solutions

Memory Map Analysis

- Section breakdown:
    - [.text section analysis]
        - Size: 000b9800
    - [.data section analysis]
        - There is no data section
    - [.rsrc section analysis]
        - Size: 004bc000
    - [Other relevant sections]
        - .reloc section:
            - Size: 004ce000
- Notable findings:
    - [Unusual section permissions]
        - none
    - [Section size anomalies]
        - none

String Analysis

I used Ghidra for strings

- Notable strings discovered:
    - [URLs/IPs]
        - 16.0.0.0

- [File paths]
    - C:\Users\Administrator\Desktop\Client\Temp\hDfjaWdXku\src\obj\Debug\StaticArrayInitTypeSize1.pdb
- [Command lines]
- [API calls]

```
Credentials not given.
WrapNonExceptionThrows
JobClock Administration Applet
BASeCamp Software Solutions
BASeCamp JobClock
2ce5239f-99b1-4921-b1e0-05ddf7544bc1
1.4.8.0
System.Resources.Tools.StronglyType
dResourceBuilder
16.0.0.0
RSDS
C:\Users\Administrator\Desktop\Clie
nt\Temp\hDfjaWdXku\src\obj\Debug\St
aticArrayInitTypeSize1.pdb
_CorExeMain
mscoree.dll
VS_VERSION_INFO
StringFileInfo
000004B0
Comments
TikTok Sensor Bypass
CompanyName
TikTok INC
FileDescription
Bypass Censorship on TikTok Platform
FileVersion
1.4.8.0
InternalName
TikTokBypassCensor.exe
LegalCopyright
Copyright ©  2025 ByteDance
Software Solutions
LegalTrademarks
2025 Professor Galde University of
Arizona
OriginalFilename
TikTokBypass.exe
ProductName
Week 3 Malware Analysis
ProductVersion
1.4.8.0
Assembly Version
1.4.8.0
```

```
VarFileInfo
_Dirty
AddDirty
IsDirty
SetDirty
CREATEDIRTYTABLE
GETISDIRTY
COUNTDIRTY
SETDIRTY
ADDDIRTY
SELECT "DIRTYBIT" FROM `DirtyData`
WHERE ID = "{0}"
UPDATE `DirtyData` SET DIRTYBIT="1"
WHERE ID="{0}"
INSERT INTO `DirtyData`
(ID,DIRTYBIT) VALUES ("{0}","{1}")
CLEARDIRTY
UPDATE `DirtyData` SET
`DIRTYBIT`="0" WHERE ID="{0}"
SELECT COUNT(*) FROM `DirtyData`
WHERE ID="{0}"
DROP TABLE IF EXISTS `DirtyData`;
CREATE TABLE `DirtyData` (`ID`
VARCHAR(64) NOT NULL,
`DIRTYBIT` BOOL NOT NULL,
 PRIMARY KEY (`ID`));
A Tech no longer has active work
orders.
Job Monitor will continue to run in
the background. To reopen it, click
this icon.
 Comments.
Cyclical INCLUDE's detected in INI
file.
 not enumerated...
Assembly enumeration complete.(
 Assemblies.
Assembly enumeration complete.
Removing duplicates...
ConnectionString=Provider=Microsoft
.Jet.OLEDB.4.0;Data Source={0}
Version:0.9
bug...
```

```
DataLayer Initializing...               client.log
Connecting to Database...               admin.log
BCJobClock\blankdb.mdb                  *.png
BCJobClock\JobClock.mdb                 Login cancelled.
BCJobClock\BCJobClock_app.log           Ticking...(
{0:00}:{1:00}:{2:00}.{3:00}             Please Wait...
```

- Analysis of string findings:
  - [Potential functionality indicated]
    - presence of client.log, admin.log, and logging-related messages suggests the malware may collect and store user activity data.
    - The references to Microsoft Access databases (blankdb.mdb, JobClock.mdb) could indicate credential storage, keylogging, or tracking of system activity.
  - [Suspicious patterns]
    - Multiple references using the term DIRTY, I found odd

Entropy Analysis

- Overall entropy score: [Score]
  - Overall: 6.87705 (85% packed)
- Section-specific entropy:
  - [List sections with unusual entropy]
  - PE Header (unpacked): 1.63143
  - Section (0) ['.text'] (packed): 7.18396
- Packing analysis:
  - [Packed/Unpacked determination]
    - The text section is packed
  - [Packer identified (if applicable)]
    - I do not know what packer was used
  - [Unpacking methodology (if attempted)]
    - UnPacMe
  - [Alternative unpacking approaches (if needed)]

3. Static Analysis Summary

- Key findings from static analysis:
  - [Major indicators of malicious behavior]
    - Packed .text section with high entropy suggests the file is obfuscated to evade detection.
    - ConnectionString=Provider=Microsoft.Jet.OLEDB.4.0;Data Source={0} Microsoft Jet Database Engine is commonly used to store credentials,making it a target for malware
    - 16.0.0.0 (Possible internal or C2 IP address) Could be used for network-based communication with an attacker-controlled server.

    - [Potential functionality]
        - Credential stealing: The presence of mscoree.dll and Microsoft database drivers suggests potential credential harvesting.
        - data exfiltration, persistence, potential credential theft, and anti-analysis
    - [Risk indicators]
        - Highly suspicious packed executable
        - Multiple malware classifications (ransomware, infostealer, trojan)
        - Database manipulation and potential logging of user activity

Dynamic Analysis

1. Analysis Environment

Environment Setup

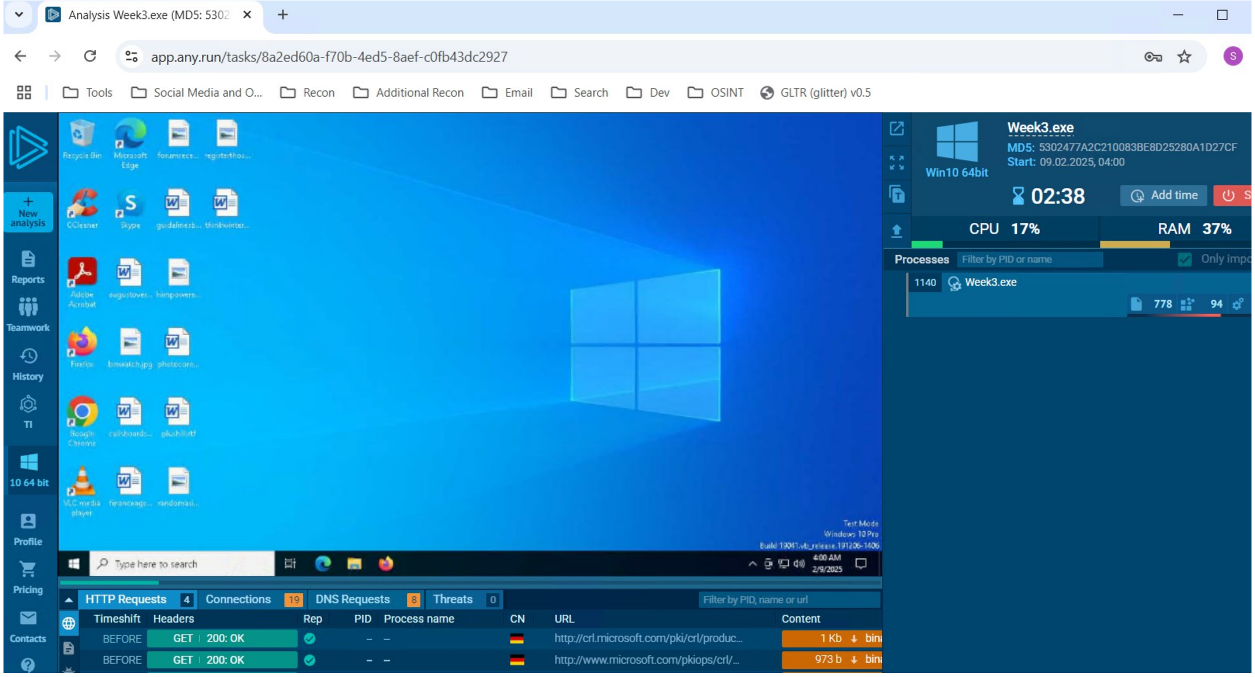
- Virtual Machine specifications:
    - [OS version] Windows 2022 Server Datacenter Version:10.0.20348 Build 20348
    - [Memory allocation]: 8GB RAM
    - [Network configuration]:Connected to internet, Network 3 Ethernet 3
        - Used fakenet
- Monitoring tools deployed:
    - [Process monitoring]
        - Ensure you use RegShot, Process Monitor, Process Explorer
        - Used RegShot and Process Monitor
    - [Network monitoring]
        - Ensure you use Wireshark
        - Used Wireshark
    - [File system monitoring]
- Safety measures implemented:
    - [Network isolation]
        - Try the analysis with and without Fakenet
    - [Snapshot configuration]
        - Reset Virtual Machine after running Week3.exe
    - [Additional protections]

2. Runtime Observations

Initial Execution

- [Immediate system changes]
    - AnyRun flagged this as Keylogger, Stealer

- [Process creation]
  - AnyRun
    - Week3.exe
    - RegSvcs.exe
    - svchost.exe
    - AccountsControlHost.exe
    - AuthHost.exe
    - PickerHost.exe



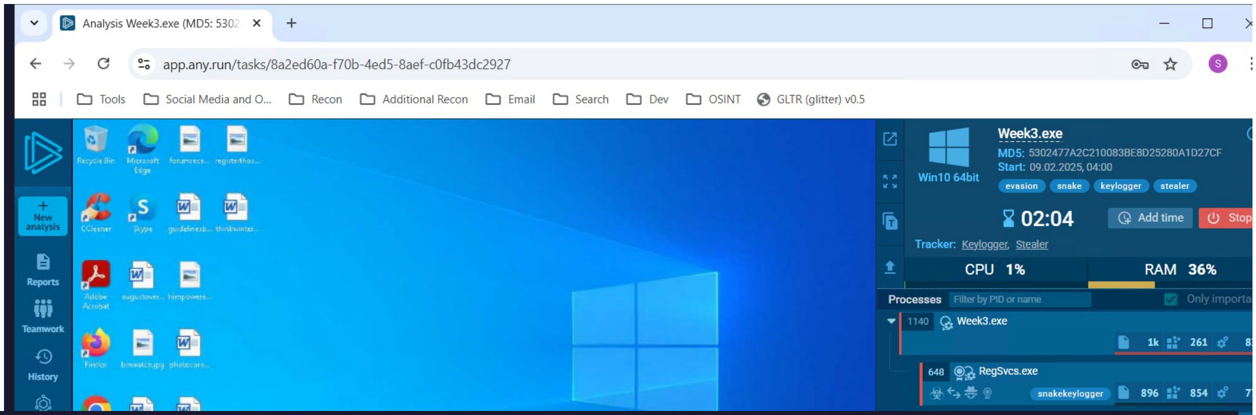
Week3.exe
MD5: 5302477A2C210083BE8D25280A1D27CF
Start: 09.02.2025, 04:00

02:38

CPU 17% RAM 37%

1140 Week3.exe 778 94

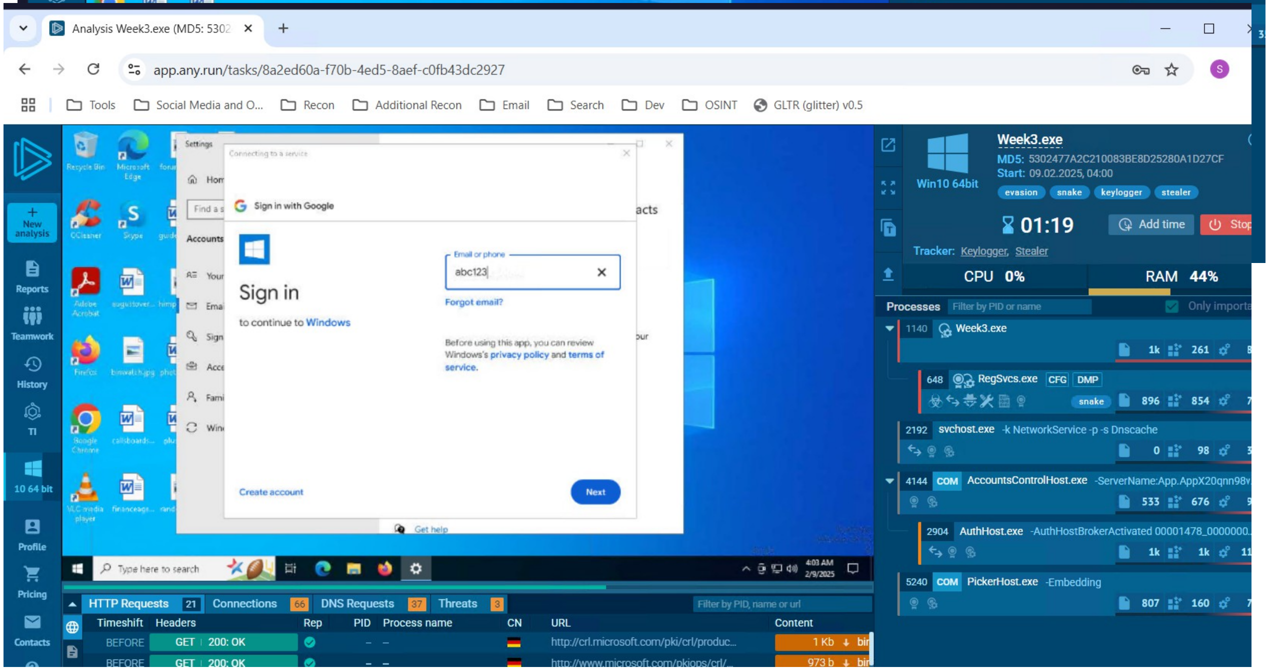
Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
BEFORE	GET 200: OK	✓	–	–	🇩🇪	http://crl.microsoft.com/pki/crl/produc...	1 Kb ↓ bina
BEFORE	GET 200: OK	✓	–	–	🇩🇪	http://www.microsoft.com/pkiops/crl/...	973 b ↓ bina



app.any.run/tasks/8a2ed60a-f70b-4ed5-8aef-c0fb43dc2927

Week3.exe
MD5: 5302477A2C210083BE8D25280A1D27CF
Start: 09.02.2025, 04:00
Win10 64bit
evasion snake keylogger stealer
02:04
Tracker: Keylogger, Stealer
CPU 1% RAM 36%

Processes
1140 Week3.exe 1k 261
648 RegSvcs.exe snakekeylogger 896 854



app.any.run/tasks/8a2ed60a-f70b-4ed5-8aef-c0fb43dc2927

Sign in with Google

Sign in
to continue to Windows

Email or phone: abc123

Forgot email?

Before using this app, you can review Windows's privacy policy and terms of service.

Create account
Next

Week3.exe
MD5: 5302477A2C210083BE8D25280A1D27CF
Start: 09.02.2025, 04:00
Win10 64bit
evasion snake keylogger stealer
01:19
Tracker: Keylogger, Stealer
CPU 0% RAM 44%

Processes
1140 Week3.exe 1k 261
648 RegSvcs.exe CFG DMP snake 896 854
2192 svchost.exe -k NetworkService -p -s Dnscache 0 98
4144 COM AccountsControlHost.exe -ServerName:App.AppX20qnn98v 533 676
2904 AuthHost.exe -AuthHostBrokerActivated 00001478_0000000 1k 1k
5240 COM PickerHost.exe -Embedding 807 160

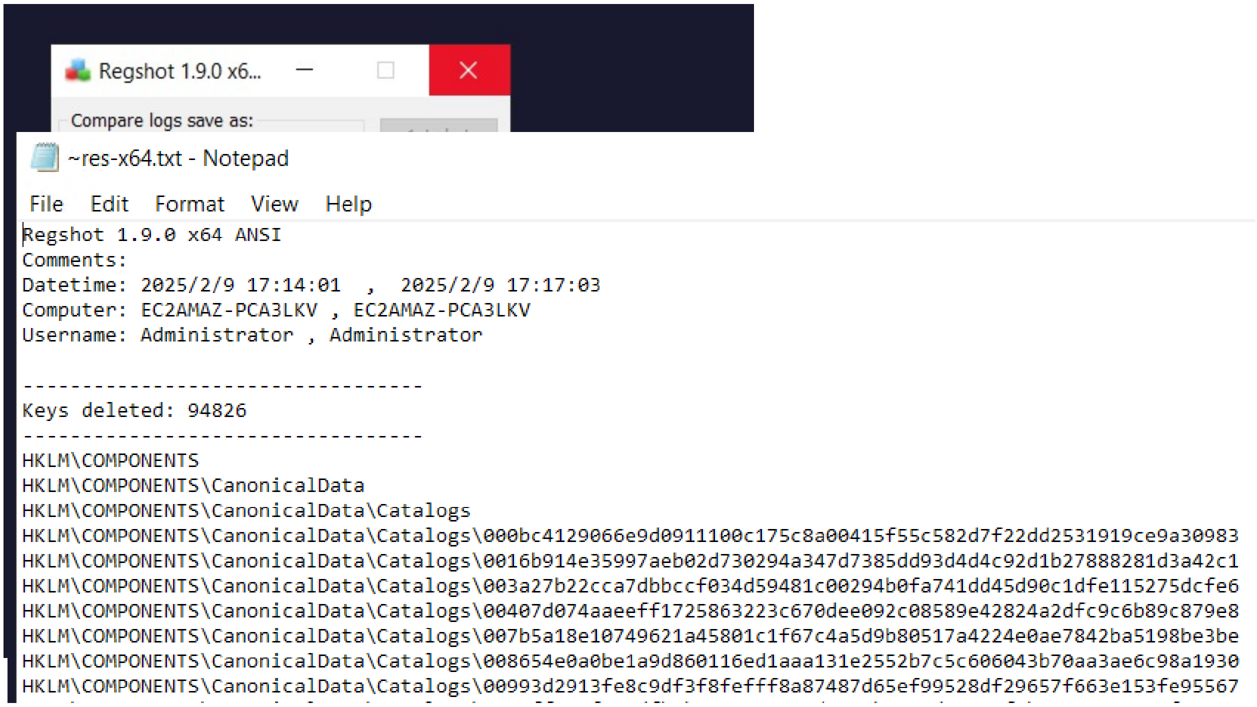
HTTP Requests 21 | Connections 66 | DNS Requests 37 | Threats 3

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
BEFORE	GET 200: OK	✓	–	–		http://crl.microsoft.com/pki/crl/produc...	1 Kb bir
BEFORE	GET 200: OK	✓	–	–		http://www.microsoft.com/pkiops/crl/...	973 b bir

Run in Virtual Machine

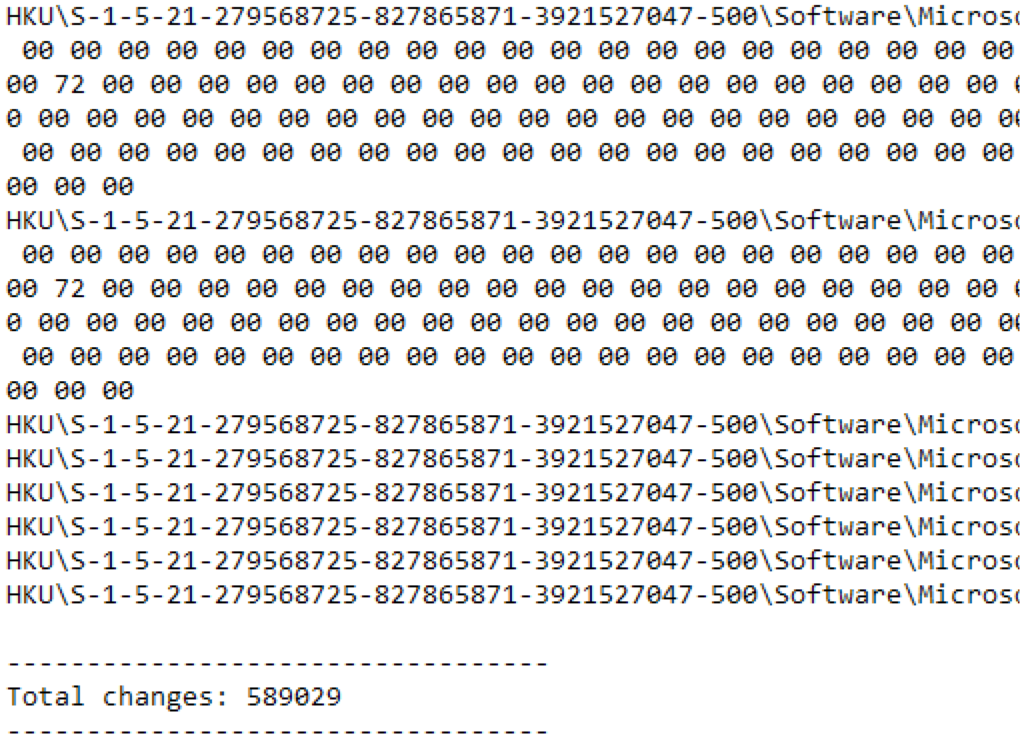
- CreateFile and QueryBasicInformation

- [Registry creation]
  - Keys changed: 25291
  - Values changed: 33455
  - Total Keys deleted: 94826
  - Total changes: 589029



```
Regshot 1.9.0 x64 ANSI
Comments:
Datetime: 2025/2/9 17:14:01  ,  2025/2/9 17:17:03
Computer: EC2AMAZ-PCA3LKV , EC2AMAZ-PCA3LKV
Username: Administrator , Administrator

----------------------------------
Keys deleted: 94826
----------------------------------
HKLM\COMPONENTS
HKLM\COMPONENTS\CanonicalData
HKLM\COMPONENTS\CanonicalData\Catalogs
HKLM\COMPONENTS\CanonicalData\Catalogs\000bc4129066e9d0911100c175c8a00415f55c582d7f22dd2531919ce9a30983
HKLM\COMPONENTS\CanonicalData\Catalogs\0016b914e35997aeb02d730294a347d7385dd93d4d4c92d1b27888281d3a42c1
HKLM\COMPONENTS\CanonicalData\Catalogs\003a27b22cca7dbbccf034d59481c00294b0fa741dd45d90c1dfe115275dcfe6
HKLM\COMPONENTS\CanonicalData\Catalogs\00407d074aaeeff1725863223c670dee092c08589e42824a2dfc9c6b89c879e8
HKLM\COMPONENTS\CanonicalData\Catalogs\007b5a18e10749621a45801c1f67c4a5d9b80517a4224e0ae7842ba5198be3be
HKLM\COMPONENTS\CanonicalData\Catalogs\008654e0a0be1a9d860116ed1aaa131e2552b7c5c606043b70aa3ae6c98a1930
HKLM\COMPONENTS\CanonicalData\Catalogs\00993d2913fe8c9df3f8fefff8a87487d65ef99528df29657f663e153fe95567
```



```
HKU\S-1-5-21-279568725-827865871-3921527047-500\Software\Micros
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00
HKU\S-1-5-21-279568725-827865871-3921527047-500\Software\Micros
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00
HKU\S-1-5-21-279568725-827865871-3921527047-500\Software\Micros
HKU\S-1-5-21-279568725-827865871-3921527047-500\Software\Micros
HKU\S-1-5-21-279568725-827865871-3921527047-500\Software\Micros
HKU\S-1-5-21-279568725-827865871-3921527047-500\Software\Micros
HKU\S-1-5-21-279568725-827865871-3921527047-500\Software\Micros
HKU\S-1-5-21-279568725-827865871-3921527047-500\Software\Micros

----------------------------------
Total changes: 589029
----------------------------------
```

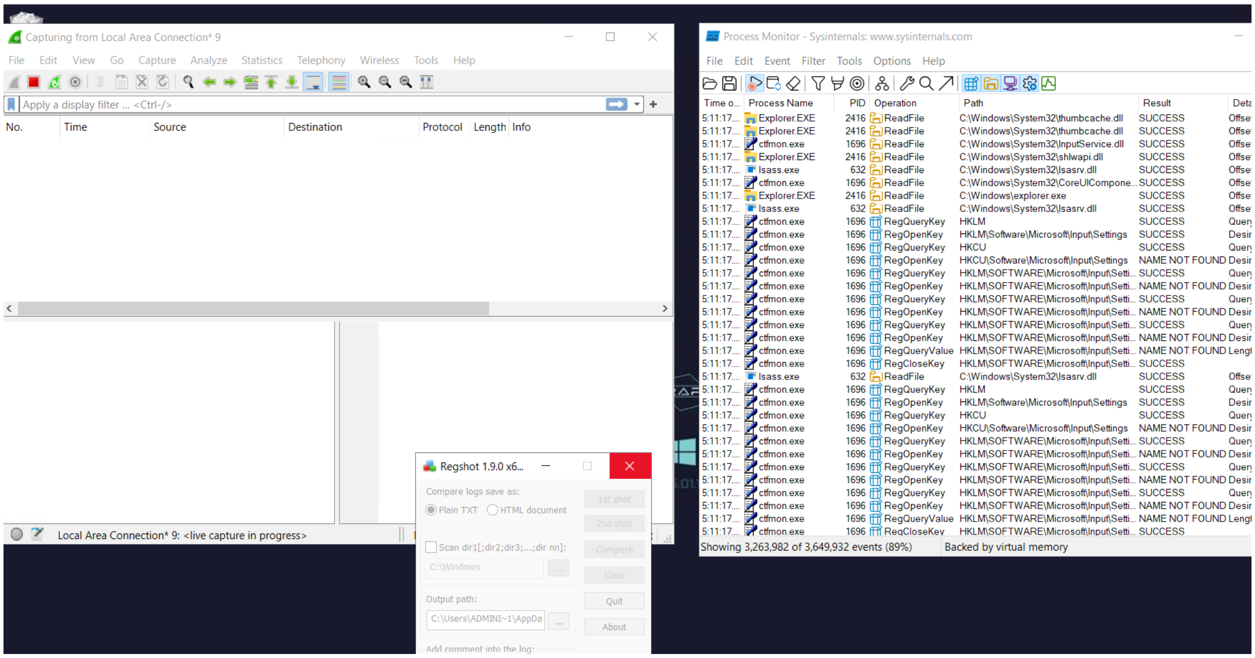
- [Network activity]
    - http://o.pki.goog/we2/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTuMJxAT2trYla

0jia%2F5EUSmLrk3QQUdb7Ed66J9kQ3fc%2BxaB8dGuvcNFkCEEQSRbXprXgTCj%2FsWFqphAQ%3D

  - Device Retrieving External IP Address Detected - RegSvcs.exe
    - ET INFO 404/Snake/Matiex Keylogger Style External IP Check
  - Wireshark: no packets captured
- [File system changes]

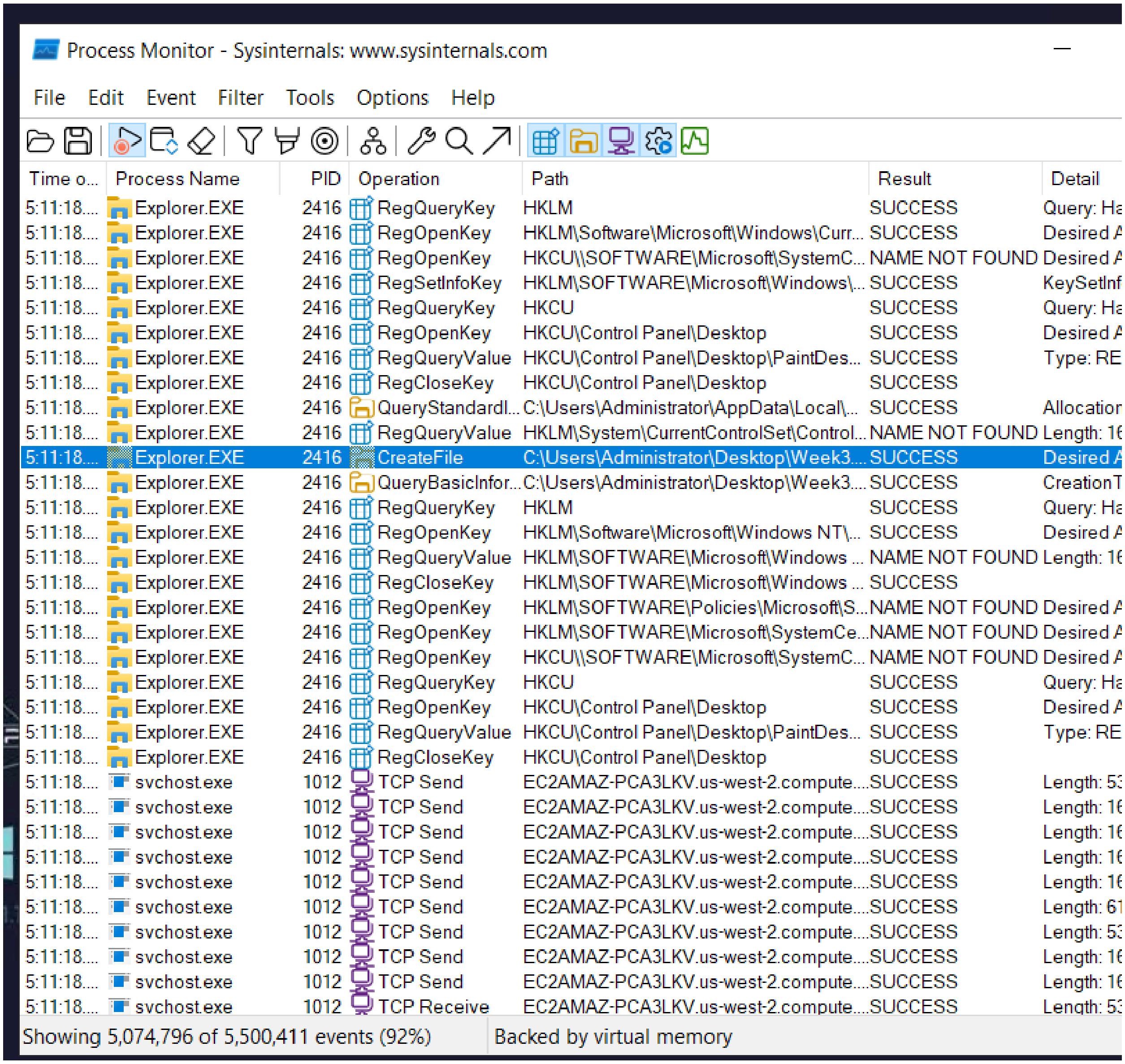
Continued Monitoring

- [Persistent changes]
  - CreateFile and QueryBasicInformation are still running
- [Scheduled tasks]
  - None
- [Registry modifications]
  - None
- [Additional payloads]


Capturing from Local Area Connection* 9
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
Local Area Connection* 9: <live capture in progress>
Regshot 1.9.0 x6...
Compare logs save as:
Plain TXT
HTML document
1st shot
2nd shot
Compare
Clear
Quit
About
Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows
Output path:
C:\Users\ADMINI~1\AppDa
Add comment into the log:
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Deta
5:11:17....	Explorer.EXE	2416	ReadFile	C:\Windows\System32\thumbcache.dll	SUCCESS	Offse
5:11:17....	Explorer.EXE	2416	ReadFile	C:\Windows\System32\thumbcache.dll	SUCCESS	Offse
5:11:17....	ctfmon.exe	1696	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS	Offse
5:11:17....	Explorer.EXE	2416	ReadFile	C:\Windows\System32\shlwapi.dll	SUCCESS	Offse
5:11:17....	lsass.exe	632	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offse
5:11:17....	ctfmon.exe	1696	ReadFile	C:\Windows\System32\CoreUICompone...	SUCCESS	Offse
5:11:17....	Explorer.EXE	2416	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offse
5:11:17....	lsass.exe	632	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offse
5:11:17....	ctfmon.exe	1696	RegQueryKey	HKLM	SUCCESS	Query
5:11:17....	ctfmon.exe	1696	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desir
5:11:17....	ctfmon.exe	1696	RegQueryKey	HKCU	SUCCESS	Query
5:11:17....	ctfmon.exe	1696	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desir
5:11:17....	ctfmon.exe	1696	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Query
5:11:17....	ctfmon.exe	1696	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	NAME NOT FOUND	Desir
5:11:17....	ctfmon.exe	1696	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Query
5:11:17....	ctfmon.exe	1696	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	NAME NOT FOUND	Desir
5:11:17....	ctfmon.exe	1696	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Query
5:11:17....	ctfmon.exe	1696	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	NAME NOT FOUND	Desir
5:11:17....	ctfmon.exe	1696	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Setti...	NAME NOT FOUND	Lengt
5:11:17....	ctfmon.exe	1696	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	
5:11:17....	lsass.exe	632	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offse
5:11:17....	ctfmon.exe	1696	RegQueryKey	HKLM	SUCCESS	Query
5:11:17....	ctfmon.exe	1696	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desir
5:11:17....	ctfmon.exe	1696	RegQueryKey	HKCU	SUCCESS	Query
5:11:17....	ctfmon.exe	1696	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desir
5:11:17....	ctfmon.exe	1696	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Query
5:11:17....	ctfmon.exe	1696	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	NAME NOT FOUND	Desir
5:11:17....	ctfmon.exe	1696	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Query
5:11:17....	ctfmon.exe	1696	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	NAME NOT FOUND	Desir
5:11:17....	ctfmon.exe	1696	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Query
5:11:17....	ctfmon.exe	1696	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	NAME NOT FOUND	Desir
5:11:17....	ctfmon.exe	1696	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Setti...	NAME NOT FOUND	Lengt
5:11:17....	ctfmon.exe	1696	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	

Showing 3,263,982 of 3,649,932 events (89%) Backed by virtual memory


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
5:11:18....	Explorer.EXE	2416	RegQueryKey	HKLM	SUCCESS	Query: Ha
5:11:18....	Explorer.EXE	2416	RegOpenKey	HKLM\Software\Microsoft\Windows\Curr...	SUCCESS	Desired A
5:11:18....	Explorer.EXE	2416	RegOpenKey	HKCU\\SOFTWARE\Microsoft\SystemC...	NAME NOT FOUND	Desired A
5:11:18....	Explorer.EXE	2416	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	KeySetInf
5:11:18....	Explorer.EXE	2416	RegQueryKey	HKCU	SUCCESS	Query: Ha
5:11:18....	Explorer.EXE	2416	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired A
5:11:18....	Explorer.EXE	2416	RegQueryValue	HKCU\Control Panel\Desktop\PaintDes...	SUCCESS	Type: RE
5:11:18....	Explorer.EXE	2416	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
5:11:18....	Explorer.EXE	2416	QueryStandardI...	C:\Users\Administrator\AppData\Local\...	SUCCESS	Allocatior
5:11:18....	Explorer.EXE	2416	RegQueryValue	HKLM\System\CurrentControlSet\Control...	NAME NOT FOUND	Length: 16
5:11:18....	Explorer.EXE	2416	CreateFile	C:\Users\Administrator\Desktop\Week3....	SUCCESS	Desired A
5:11:18....	Explorer.EXE	2416	QueryBasicInfor...	C:\Users\Administrator\Desktop\Week3....	SUCCESS	CreationT
5:11:18....	Explorer.EXE	2416	RegQueryKey	HKLM	SUCCESS	Query: Ha
5:11:18....	Explorer.EXE	2416	RegOpenKey	HKLM\Software\Microsoft\Windows NT\...	SUCCESS	Desired A
5:11:18....	Explorer.EXE	2416	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows ...	NAME NOT FOUND	Length: 16
5:11:18....	Explorer.EXE	2416	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows ...	SUCCESS	
5:11:18....	Explorer.EXE	2416	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\S...	NAME NOT FOUND	Desired A
5:11:18....	Explorer.EXE	2416	RegOpenKey	HKLM\SOFTWARE\Microsoft\SystemCe...	NAME NOT FOUND	Desired A
5:11:18....	Explorer.EXE	2416	RegOpenKey	HKCU\\SOFTWARE\Microsoft\SystemC...	NAME NOT FOUND	Desired A
5:11:18....	Explorer.EXE	2416	RegQueryKey	HKCU	SUCCESS	Query: Ha
5:11:18....	Explorer.EXE	2416	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired A
5:11:18....	Explorer.EXE	2416	RegQueryValue	HKCU\Control Panel\Desktop\PaintDes...	SUCCESS	Type: RE
5:11:18....	Explorer.EXE	2416	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
5:11:18....	svchost.exe	1012	TCP Send	EC2AMAZ-PCA3LKV.us-west-2.compute....	SUCCESS	Length: 53
5:11:18....	svchost.exe	1012	TCP Send	EC2AMAZ-PCA3LKV.us-west-2.compute....	SUCCESS	Length: 16
5:11:18....	svchost.exe	1012	TCP Send	EC2AMAZ-PCA3LKV.us-west-2.compute....	SUCCESS	Length: 16
5:11:18....	svchost.exe	1012	TCP Send	EC2AMAZ-PCA3LKV.us-west-2.compute....	SUCCESS	Length: 16
5:11:18....	svchost.exe	1012	TCP Send	EC2AMAZ-PCA3LKV.us-west-2.compute....	SUCCESS	Length: 16
5:11:18....	svchost.exe	1012	TCP Send	EC2AMAZ-PCA3LKV.us-west-2.compute....	SUCCESS	Length: 61
5:11:18....	svchost.exe	1012	TCP Send	EC2AMAZ-PCA3LKV.us-west-2.compute....	SUCCESS	Length: 53
5:11:18....	svchost.exe	1012	TCP Send	EC2AMAZ-PCA3LKV.us-west-2.compute....	SUCCESS	Length: 16
5:11:18....	svchost.exe	1012	TCP Send	EC2AMAZ-PCA3LKV.us-west-2.compute....	SUCCESS	Length: 16
5:11:18....	svchost.exe	1012	TCP Receive	EC2AMAZ-PCA3LKV.us-west-2.compute....	SUCCESS	Length: 53

Showing 5,074,796 of 5,500,411 events (92%) Backed by virtual memory

3. Post-Execution Analysis
   - System state changes:
     - [Permanent modifications]
       - Processes from Week3.exe continued to run
     - [Persistence mechanisms]
       - Not sure
     - [Data exfiltration evidence]
       - presence of client.log, admin.log, and logging-related

messages suggests the malware may collect and store user activity data.

- Network activity summary:
    - [Connection attempts]
        - none
    - [Data transfers]
        - none
    - [Command & Control activity]
        - none

Impact Analysis

1. User Impact Assessment

Home Users

- [Potential impact]:
    - sensitive information such as passwords, browsing history, and user activity logs may be exfiltrated
- [Risk level]
    - High – the malware steals credentials and logs user input
- [Data compromise potential]
    - interacts with database files that may store credentials

Business Users

- [Operational disruption potential]
    - Could lead to unauthorized access

2. Mitigation Strategy

Immediate Response

- [Initial containment steps]
    - isolate infected systems from the network
- [System isolation procedures]
    - remove the infected device from all internal networks
- [Data preservation methods]
    - collect log files and registry changes for forensic analysis

Long-term Prevention

- [Security control recommendations]\
    - update and patch systems
- [Policy modifications]
    - increase security awareness training on phishing
- [Training requirements]
    - Provide malware analysis training

Conclusion

1. Analysis Reflection

- [Summary of findings]
    - malware is a suspicious packed executable with indications of credential theft and keylogging
- [Unusual characteristics]
    - Microsoft Jet Database Engine indicates credential theft.
    - High entropy in the .text section indicates packing
    - Database-related functions imply keylogging or credential theft
- [Learning outcomes]
    - Static analysis shows that malware is packed, indicating obfuscation
    - Dynamic execution revealed logging indicating possible keylogging
- [Additional research needed]

2. Evidence Documentation

- [Screenshot descriptions and relevance]
    - See screenshots above
- [Tool output documentation]
    - Ghidra, Detect It Easy, VirusTotal, AnyRun, Process Monitor, Wireshark, Regshot
- [Additional supporting materials]