Kaspersky ICS CERT

kaspersky

PseudoManuscrypt: a mass-scale spyware attack campaign

Kaspersky ICS CERT

16.12.2021

Version 1.1

In June 2021, Kaspersky ICS CERT experts identified malware whose loader has some similarities to the Manuscrypt malware, which is part of the Lazarus APT group's arsenal. In 2020, the group used Manuscrypt in attacks on defense enterprises in different countries. These attacks are described in the report "Lazarus targets defense industry with ThreatNeedle".

Curiously, the data exfiltration channel of the malware uses an implementation of the KCP protocol that has previously been seen in the wild only as part of the APT41 group's toolset.

We dubbed the newly-identified malware PseudoManuscrypt.

The PseudoManuscrypt loader makes its way onto user systems via a MaaS platform that distributes malware in pirated software installer archives. One specific case of the PseudoManuscrypt downloader's distribution is its installation via the Glupteba botnet (whose main installer is also distributed via the pirated software installer distribution platform). This means that the malware distribution tactics used by the threat actor behind PseudoManuscrypt demonstrate no particular targeting.

During the period from January 20 to November 10, 2021, Kaspersky products blocked PseudoManuscrypt on more than 35,000 computers in 195 countries of the world. Such a large number of attacked systems is not characteristic of the Lazarus group or APT attacks as a whole.

Targets of PseudoManuscrypt attacks include a significant number of industrial and government organizations, including enterprises in the military-industrial complex and research laboratories.

According to our telemetry, at least 7.2% of all computers attacked by the PseudoManuscrypt malware are part of industrial control systems (ICS) used by organizations in various industries, including Engineering, Building Automation, Energy, Manufacturing, Construction, Utilities, and Water Management.

The main PseudoManuscrypt module has extensive and varied spying functionality. It includes stealing VPN connection data, logging keypresses, capturing screenshots and videos of the screen, recording sound with the microphone, stealing clipboard data and operating system event log data (which also makes stealing RDP authentication data possible), and much more. Essentially, the functionality of PseudoManuscrypt provides the attackers with virtually full control of the infected system.

The full report is available on the Kaspersky Threat Intelligence portal.
For more information please contact: ics-cert@kaspersky.com.

Technical details

Identifying the loader. General information

In June 2021, Kaspersky ICS CERT experts uncovered a series of attacks targeting organizations across the globe, including government organizations and industrial enterprises.

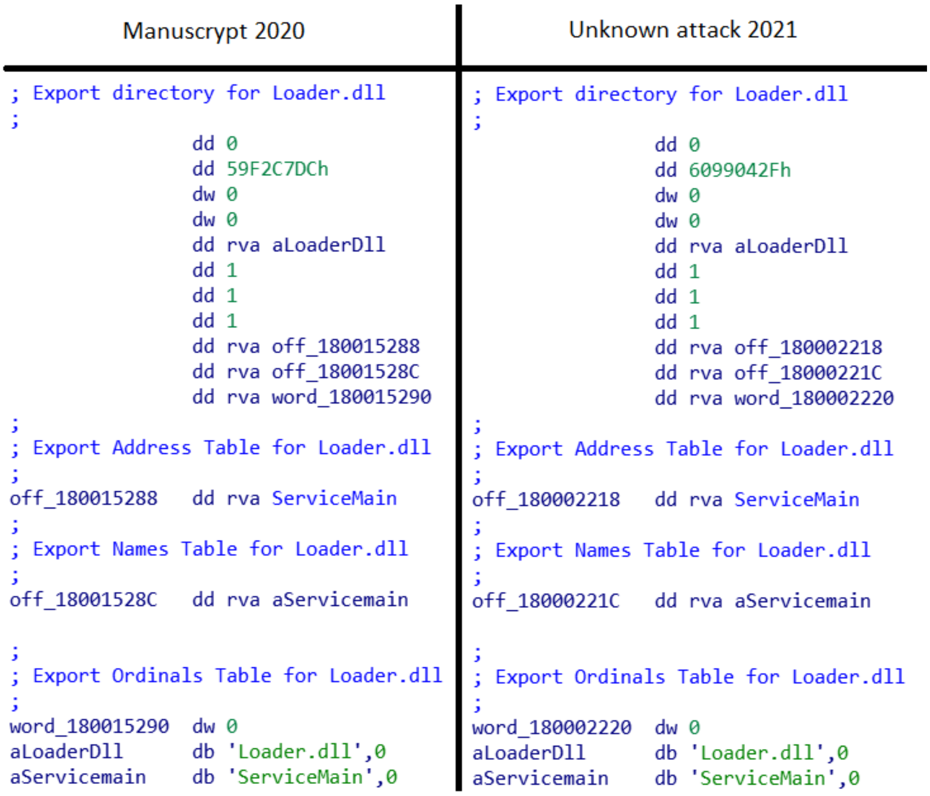
Initially, the malware was detected when it triggered antivirus solutions' detection logic designed to detect the activity of the Lazarus APT. However, the overall picture of what was going on was too unusual to link the malicious activity to Lazarus. Specifically, the newly-identified malware had attacked at least 35,000 systems, which is uncharacteristic of a targeted attack.

Research has revealed that the malware used in the attack loads its payload from the system registry and decrypts it. The payload's location in the registry is unique for each infected system.

The newly-identified malware loader has some similarities to the loader used by the Manuscrypt malware, which was used by the Lazarus group in 2020 to attack defense enterprises in different countries. (More detailed information on the attack can be found in the following report: "Lazarus Targets Defense Industry with ThreatNeedle".)

Both malicious programs load a payload from the system registry and decrypt it; in both cases, a special value in the CLSID format is used to determine the payload's location in the registry.

The executable files of both malicious programs have virtually identical export tables:



Manuscrypt 2020

```
; Export directory for Loader.dll
;
                dd 0
                dd 59F2C7DCh
                dw 0
                dw 0
                dd rva aLoaderDll
                dd 1
                dd 1
                dd 1
                dd rva off_180015288
                dd rva off_18001528C
                dd rva word_180015290
;
; Export Address Table for Loader.dll
;
off_180015288   dd rva ServiceMain
;
; Export Names Table for Loader.dll
;
off_18001528C   dd rva aServicemain

;
; Export Ordinals Table for Loader.dll
;
word_180015290  dw 0
aLoaderDll      db 'Loader.dll',0
aServicemain    db 'ServiceMain',0
```

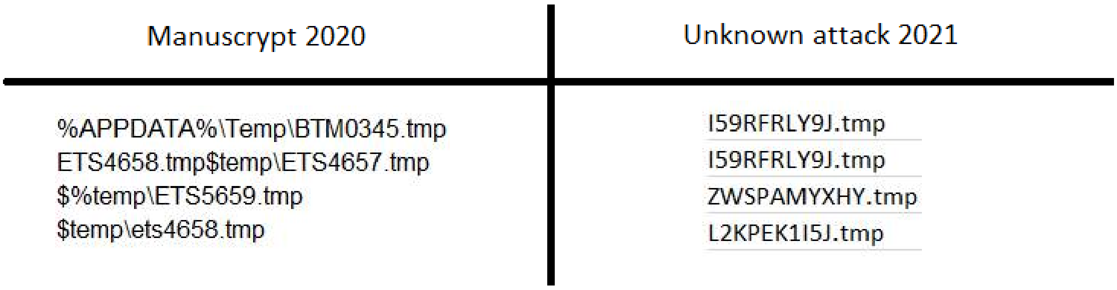
Unknown attack 2021

```
; Export directory for Loader.dll
;
                dd 0
                dd 6099042Fh
                dw 0
                dw 0
                dd rva aLoaderDll
                dd 1
                dd 1
                dd 1
                dd rva off_180002218
                dd rva off_18000221C
                dd rva word_180002220
;
; Export Address Table for Loader.dll
;
off_180002218   dd rva ServiceMain
;
; Export Names Table for Loader.dll
;
off_18000221C   dd rva aServicemain

;
; Export Ordinals Table for Loader.dll
;
word_180002220  dw 0
aLoaderDll      db 'Loader.dll',0
aServicemain    db 'ServiceMain',0
```

Comparison of the two malicious programs' export tables

In addition, the two malicious programs use similar executable file naming formats:



Manuscrypt 2020	Unknown attack 2021
%APPDATA%\Temp\BTM0345.tmp	I59RFRLY9J.tmp
ETS4658.tmp$temp\ETS4657.tmp	I59RFRLY9J.tmp
$%temp\ETS5659.tmp	ZWSPAMYXHY.tmp
$temp\ets4658.tmp	L2KPEK1I5J.tmp

Executable file names

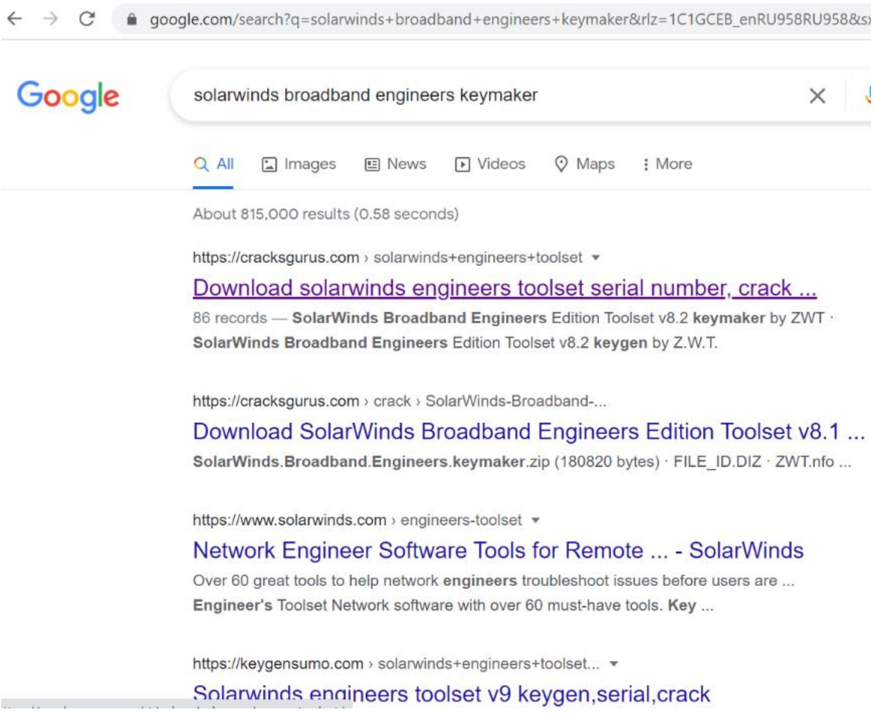
To emphasize the similarity of the newly-identified malware with Manuscrypt, while at the same time there was nothing else to link it to the Lazarus group, we decided to dub the Trojan PseudoManuscrypt.

System infection

The PseudoManuscrypt loader makes its way onto a user system via complicated chains of numerous other malicious files' installations and the creation of many different processes. These chains are diverse, but they all begin with fake pirated software installer archives. Examples of archive names, which contain references to software of diverse types and purposes, are provided below:

```
microsoft_office_365_july_keygen_by_keygensumo.zip
windows_10_pro_full_keygen_by_keygensumo.zip
adobe_acrobat_v8_0_keygen_by_keygensumo.zip
garmin_1_serial_keygen.zip
call_of_duty_black_ops_keygen_by_keygensumo.zip
kaspersky_antivirus_keys_july_keygen_by_keygensumo
solarwinds_broadband_engineers_keymaker.zip
modscan32_v8_a00_crack.zip
```

It is worth noting that these archives include fake installers of ICS-specific software, such as an application designed to create a MODBUS Master Device to receive data from a PLC, as well as more general-purpose software, which is nevertheless used on OT networks, such as a key generator for a SolarWinds tool for network engineers and systems administrators.


google.com/search?q=solarwinds+broadband+engineers+keymaker&rlz=1C1GCEB_enRU958RU958&s
Google
All
Images
News
Videos
Maps
More

solarwinds broadband engineers keymaker

About 815,000 results (0.58 seconds)

https://cracksgurus.com › solarwinds+engineers+toolset ▾
Download solarwinds engineers toolset serial number, crack ...
86 records — **SolarWinds Broadband Engineers** Edition Toolset v8.2 **keymaker** by ZWT · **SolarWinds Broadband Engineers** Edition Toolset v8.2 **keygen** by Z.W.T.

https://cracksgurus.com › crack › SolarWinds-Broadband-...
Download SolarWinds Broadband Engineers Edition Toolset v8.1 ...
SolarWinds.Broadband.Engineers.keymaker.zip (180820 bytes) · FILE_ID.DIZ · ZWT.nfo ...

https://www.solarwinds.com › engineers-toolset ▾
Network Engineer Software Tools for Remote ... - SolarWinds
Over 60 great tools to help network **engineers** troubleshoot issues before users are ... **Engineer's** Toolset Network software with over 60 must-have tools. **Key** ...

https://keygensumo.com › solarwinds+engineers+toolset... ▾
Solarwinds engineers toolset v9 keygen,serial,crack

Malicious web pages with installers in search-engine results

Resources used to distribute such installers can be found in top positions on search engine results pages. This indicates that the attackers are actively performing search-engine optimization for these resources.

Execution flow

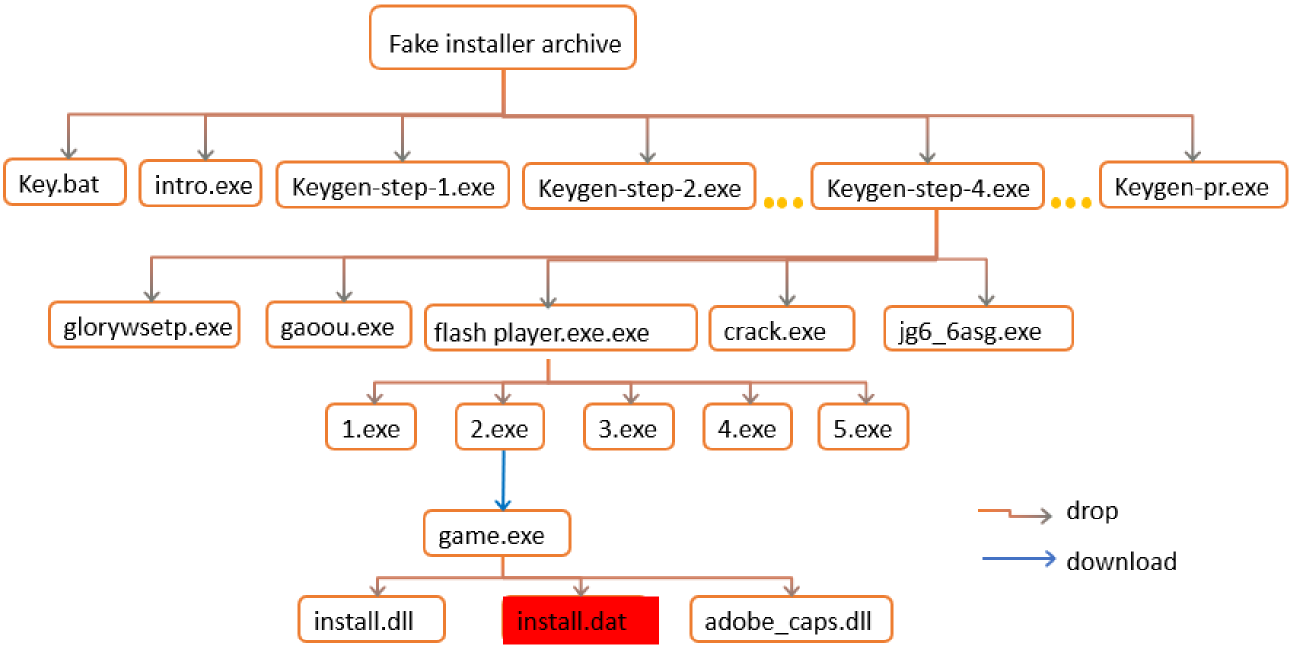
There are numerous possible variants of the execution flow of a sequence of different malicious programs leading to PseudoManuscrypt installation.

In addition to the file analyzed in this paper, malware installers download and execute numerous other malicious programs, including spyware, backdoors, cryptocurrency miners, and adware.

At each stage, we detected a large number of different droppers installed and modules downloaded, with the data theft functionality duplicated in different modules and with each module using its own command-and-control servers. This could indicate that the installers are offered by threat actors via a MaaS platform, possibly to many operators of different malicious campaigns, one of which is apparently the PseudoManuscrypt distribution campaign.

The examples and graph fragments shown below illustrate the process chains leading to PseudoManuscrypt installation.

Variant 1.



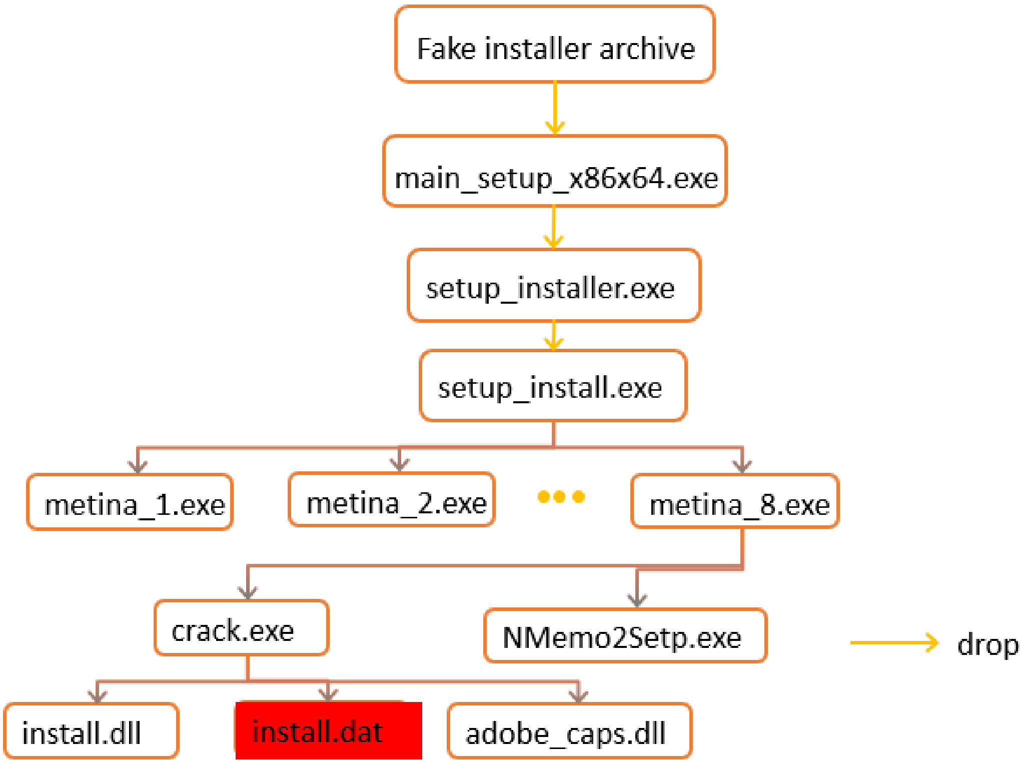
Execution flow, variant 1

In the first variant:

- the file key.bat is extracted from a fake installer,
- key.bat executes Keygen-step-4.exe (e41826b342686c7f879474c49c7eed98),
- Keygen-step-4.exe installs and executes flash player.exe (2aab0ec738374db4e872812a84a0bc11),
- flash player.exe installs and executes 2.exe (8b9f6b0c98c0afdd75c2322f1ca4d0e8).

The file 2.exe uses the link hxxps://google[.]diragame[.]com/userf/3002/gogonami.exe to download the main PseudoManuscrypt module – game.exe (0001759655eacb4e57bdf5e49c6e7585).

Variant 2.



Execution flow, variant 2

In the second variant:

- the file main_setup_x86x64.exe (1fecb6eb98e8ee72bb5f006dd79c6f2f) is extracted from a fake installer,
- main_setup_x86x64.exe installs and executes setup_installer.exe (5de2818ced29a1fedb9b24c1044ebd45),

- setup_installer.exe installs and executes setup_install.exe (58efaf6fa04a8d7201ab19170785ce85).
- setup_install.exe installs and executes the file metina_8.exe (839e9e4d6289eba53e40916283f73ca6).

The file metina_8.exe extracts and executes PseudoManuscrypt – crack.exe (89c8e5a1e24f05ede53b1cab721c53d8).

This variant involves the Glupteba infrastructure and malware installers (such as setup_installer.exe). The Glupteba botnet has been known to researchers since 2011. It is a multi-module platform that has at different times downloaded adware, spyware, cryptocurrency miners, ransomware, spam modules, and other software traditionally associated with cybercriminal activities. The Glupteba platform is quite complicated and includes numerous different modules, such as exploits for various vulnerabilities, including exploits for routers, as well as rootkits. This is why rootkits, modules of the EternalBlue exploit, and other Glupteba modules are found on computers infected with PseudoManuscrypt via the Glupteba botnet.

In another variant, which was described by BitDefender, a PseudoManuscrypt installer (8acd95006ac6d1eabf37683d7ce31052) was downloaded using the link hxxps://jom[.]diregame[.]live/userf/2201/google-game.exe – according to our telemetry, at least on May 17, 2021. It is worth noting that at different times the link could be used to download malware from different families.

Searching for other components of the malware

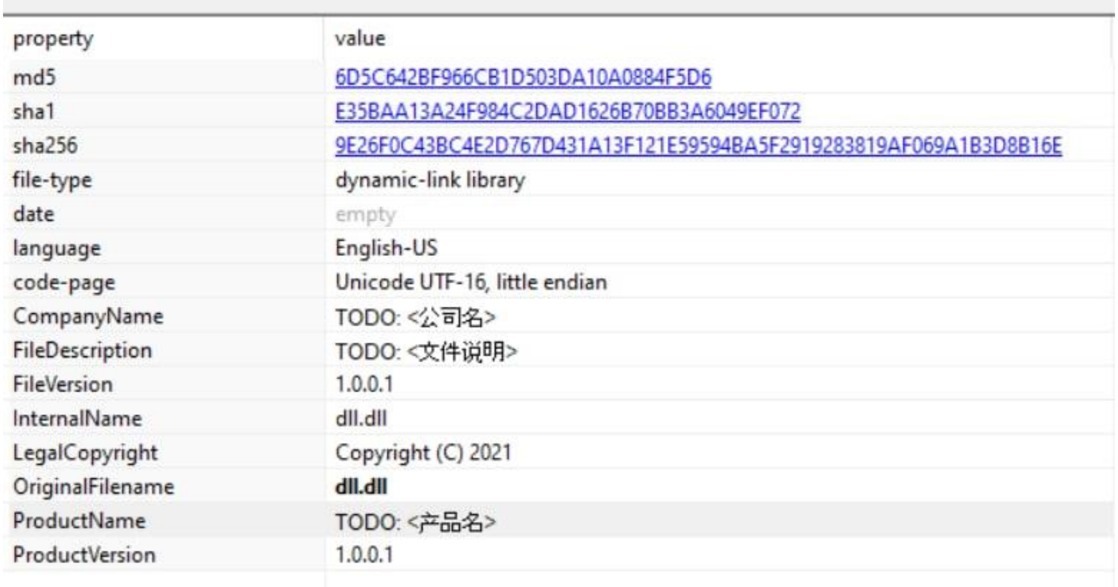
In the course of searching for other components and versions of the malware, we were able to find over 100 different versions of the PseudoManuscrypt loader.

According to our telemetry data, the mass distribution of the loader variant described in this paper began on May 10, 2021. However, its early variants were first identified on March 27, 2021, long before the attack started.

Most of the files identified in March were 'test builds'. The developer removed parts of the malicious program's code one after another, apparently trying to find out which parts of the code trigger detection by antivirus solutions.

Around the same time, the developer of the malware added dynamic import of the VirtualAlloc function. The function is used to allocate the memory needed to store the payload, which is loaded from the system registry.

Curiously, some test builds of the loader contained comments in the executable file's metadata fields. These comments were written in Chinese, which indicates that the malware developer may speak and write Chinese:



property	value
md5	6D5C642BF966CB1D503DA10A0884F5D6
sha1	E35BAA13A24F984C2DAD1626B70BB3A6049EF072
sha256	9E26F0C43BC4E2D767D431A13F121E59594BA5F2919283819AF069A1B3D8B16E
file-type	dynamic-link library
date	empty
language	English-US
code-page	Unicode UTF-16, little endian
CompanyName	TODO: <公司名>
FileDescription	TODO: <文件说明>
FileVersion	1.0.0.1
InternalName	dll.dll
LegalCopyright	Copyright (C) 2021
OriginalFilename	**dll.dll**
ProductName	TODO: <产品名>
ProductVersion	1.0.0.1

Metadata in the executable file of the malware

Main component of the malware

Finally, we were able to identify the main module of PseudoManuscrypt, whose functionality includes installing the malware on the system and which contains a payload that gives us an idea of the types of data that are of interest to the threat actor.

Installation

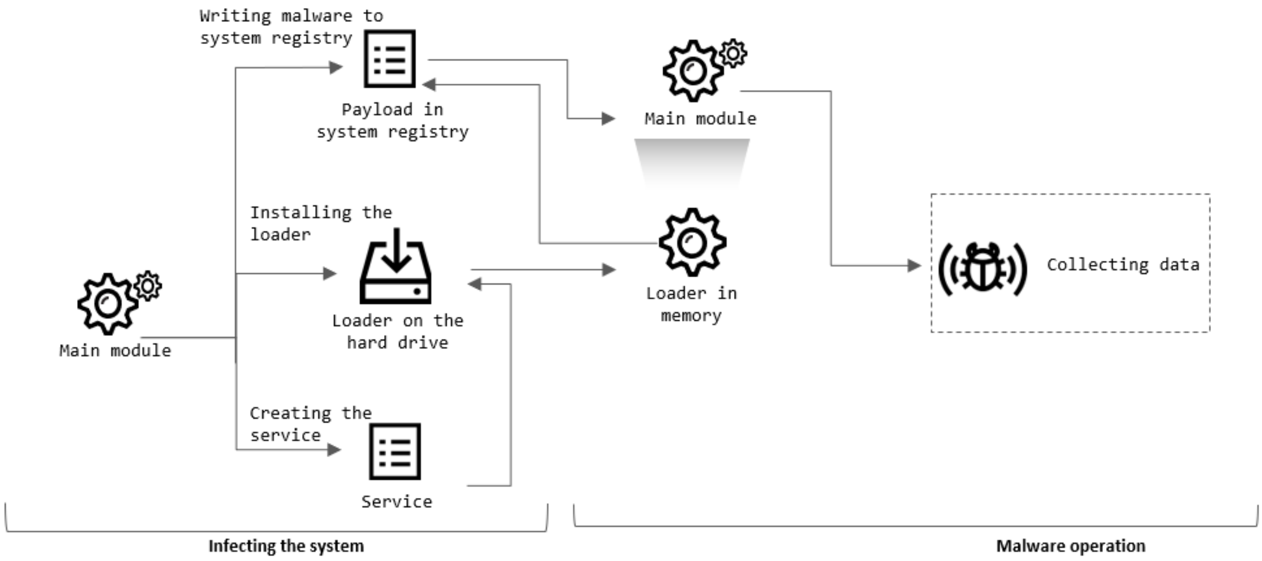
The main module of the malware writes its code to a special registry value in the HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID key. The value name (CLSID value) is unique for each system, since it is generated using the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid, which contains the system's unique identifier. The malicious program's code is stored in the system registry in encrypted form.

Next, the malware extracts, to the %TEMP% folder or the %WinDir% folder (depending on the malware modification), the loader component, which is a DLL library and has a random file name in the [0-Z]{10}.tmp format, e.g., I59RFRLY9J.tmp.

To ensure that the payload is automatically executed after system startup, the Trojan creates a service, which has the loader component as its executable file. In the earliest malware samples found, the service created by the malware had the name AppService.

Finally, the malware adds itself to the exclusions list of the Windows Defender antivirus solution by modifying the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths.

After this and, subsequently, after system restarts, the malware loader is executed. Using the value of the MachineGuid key to determine the location of the payload in the system registry, the loader loads, decrypts and executes the main component of the malware.



Malware installation and execution

Destructive activity, version 1

The first variant of the PseudoManuscrypt main module to be identified includes several modules which have the common goal of stealing confidential information from the victim's computer.

1. Keylogger. Enables the malware to intercept the codes of keys pressed by the user on the keyboard. In addition to the key codes, the malware also records the name of the application window in which the data was entered, as well as the date and time when the information was entered. The threat actor borrowed this malicious component from other

malware – Fabookie (Trojan.Win32.Fabookie), which has several modules for stealing authentication credentials for various services and websites.

The authors of PseudoManuscrypt borrowed only the keylogger module from Fabookie, ignoring the modules designed for monetizing the attack in the quickest possible way, e.g., the module for stealing bank details from web pages. This offers an insight, albeit indirect, into the goals of the attack.

2. Stealing data from the clipboard. Enables the attackers to intercept information copied by the user who works on an infected system.

3. Stealing VPN connection data. The malware gets the contents of the Windows service files used to store data on VPN connections configured on the infected system:

   %UserProfile%\Application Data\Microsoft\Network\Connections\pbk\rasphone.pbk

   %ProgramData%\Microsoft\Network\Connections\pbk\rasphone.pbk

   The Trojan attempts to extract the following data from the above files:

   - Address of the server to which to connect
   - Login and password, if they have been saved

   It is worth emphasizing the fact that different components of the malware operate at the same time, providing the attackers with information from different sources. The attackers can combine that information and use all of it together.

   For example, the malware can get the VPN server address saved in connection parameters from the file rasphone.pbk. At the same time, the login and password required to connect can be intercepted by the keylogger module. If the user copies the connection parameters using the clipboard, the data will be intercepted by the relevant module of the malware.

4. In addition to stealing VPN connection data, PseudoManuscrypt functionality includes reading Windows Application, System, and Security event logs. It cannot be said for sure what the threat actor uses the data from operating system log files for, but, in theory, it can be used (in conjunction with other bits of the PseudoManuscrypt functionality) to steal authentication data for RDP. This looks quite reasonable since the malware has VPN credential-stealing capabilities.

5. Recording sound from microphones connected to an infected system. This feature is activated upon command from the malware command-and-control server.

Destructive activity, version 2

A second variant of the malware was discovered in July 2021. The threat actor had added extended spying functionality to that variant. The following modules were added:

1. Capturing videos from the computer's screen. This feature works in conjunction with other modules designed to intercept information, such as the keylogger and the module that steals data from the clipboard. Capturing screen videos enables the attackers to see which fields the user filled in and in which windows, as well as to follow the cursor's movement and see on what areas the user clicked with the mouse.

   The module's features that are worth mentioning include transparent window support (the aero peek technology) and video compression using the GNU GPL XviD 1.3.0 codec.

2. Stealing authentication credentials from QQ and WeChat messaging applications, which are popular in Asia.

3. Collecting detailed system information: Windows version, build number, Service Pack, information on installed updates and the Windows edition, as well as the system's role, e.g., whether the system performs the domain controller function.

4. Collecting network connection data. The malware collects the names of network adapters, as well as connection type information (wired connection, Wi-Fi, fiber-optic connection, etc.).

5. Disabling antivirus solutions. The malware attempts to gain the SeDebugPrivilege privileges and terminate the following processes of security solutions:

   sepWscSvc.exe
   HipsTray.exe
   UnThreat.exe
   DF5Serve.exe
   DefenderDaemon.exe
   PowerRemind.exe
   SafeDogSiteIIS.exe
   SafeDogTray.exe
   SPIDer.exe
   f-secure.exe
   avgwdsvc.exe
   BaiduSdSvc.exe
   ServUDaemon.exe
   1433.exe
   vsserv.exe
   remupd.exe

PSafeSysTray.exe
AlilM.exe
mssecess.exe
MsMpEng.exe
QUICK HEAL
QUHLPSVC.EXE
V3Svc.exe
patray.exe
AYAgent.aye
Miner.exe
TMBMSRV.exe
knsdtray.exe
K7TSecurity.exe
QQPCTray.exe
ksafe.exe
rtvscan.exe
ashDisp.exe
avcenter.exe
kxetray.exe
egui.exe
Mcshield.exe
RavMonD.exe
KvMonXP.exe
360sd.exe
360tray.exe
DR.WEB
cfp.exe
DUB.exe
avp.exe

The malware also deletes registry keys for services belonging to security solutions whose names include the following substrings:

Symantec
UnThreat
Defender
PowerShadow
QuickHeal
F-Secure
BitDefender
Windows Defender
1433
NOD32

6. Collecting information on processes that accept network connections on TCP and UDP ports.

7. One of the PseudoManuscrypt functions removes a file named “TestDown”, which is located in the same folder as the malicious program, then it clears the URL address htt[p]://sw.bos.baidu.com/sw-search-sp/software/df60f52e0e897/qqpcmgr_12.7.18996.207_1328_0.exe from the browser’s cache, downloads a file from the above URL address again to replace the deleted file “TestDown” and sets the newly created file’s attributes to “hidden” and “system”.

8. Clearing Windows Application, Security, and System event logs.

9. Writing data received from the malware command-and-control server to the system file %System32%\drivers\etc\hosts, thereby enabling the attackers to redirect the user to malicious web resources or block access to selected sites.

10. Exchanging text messages between the command-and-control server and the malware. The malware can open a window with a chat of sorts.

The service of the new PseudoManuscrypt version is installed in the system under the name "iexplore" and has the display name "System Remote Data Simulation Layeerr". The new malware version's feature set also includes updating its executable file and removing itself from the system upon command from the malware command-and-control server.

Curiously, one of the malware samples uses the IP address 192.168.1.2 as a proxy server. This could indicate that in some cases the attackers prepare a malware sample based on the specific network architecture used by the victim.

In the new version of PseudoManuscrypt, the threat actor has also added the functionality of writing the codes of keys pressed by the user to a local log file: %System32%\9cda11af69ab0a2b6a9167f7131e7b93.key.

Finally, the new version of the Trojan sends the following HTTP headers when connecting to the malware command-and-control server:

```
HTTP/1.1

Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/x-shockwave-flash, application/vnd.ms-excel,
application/vnd.ms-powerpoint, application/msword, */*

Accept-Language: zh-cn

Accept-Encoding: gzip, deflate

User-Agent:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

Connection: Close

Cache-Control: no-cache
```

It can be seen that the malware tells the server that the preferred language of the reply is Chinese.

Sending data to the threat actor

Data collected by the malware is sent to the malware command-and-control server. In the course of our research, four such servers were identified: email.yg9[.]me, google.vrthcobj[.]com, toa.mygametoa[.]com and tob.mygametob[.]com.

The KCP protocol is used to connect to the server. According to its developers, the protocol is 10%-20% faster than TCP. The threat actor used a specific implementation of the KCP protocol.

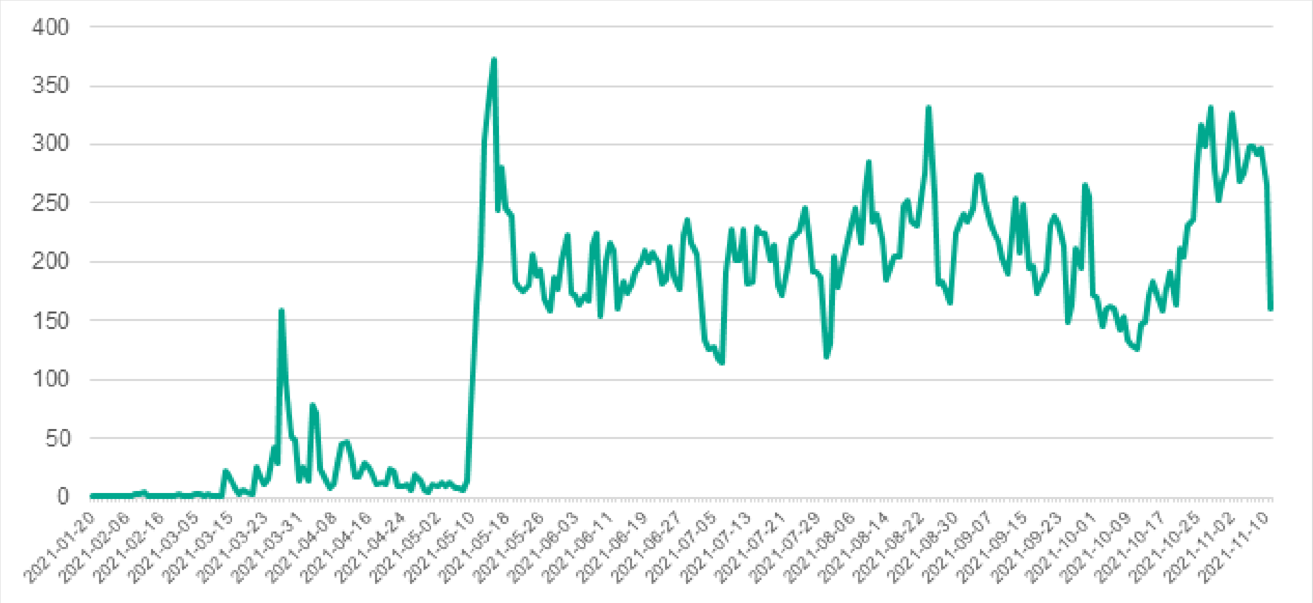
Curiously, according to a FireEye report, the KCP library used by PseudoManuscrypt malware had been used by the APT41 group in its attacks on industrial organizations from various industries, including engineering and defense industry enterprises. An analysis of malware collections that we were able to access yielded no instances of that library being used in malware other than the two cases mentioned above.

Some of the malware samples identified also use a dedicated server, d.diragame.com, to send information on new system infections. We believe that this could be a MaaS platform's statistics collection mechanism.

Victims

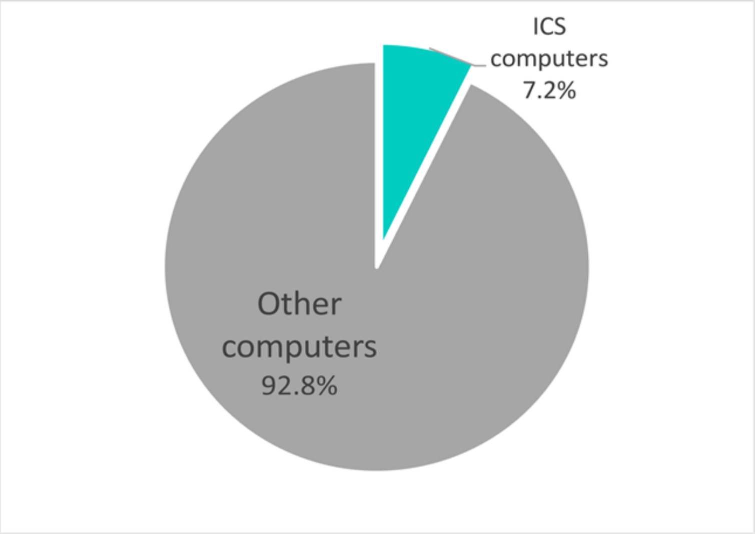
During the period from January 20 to November 10, 2021, Kaspersky products blocked PseudoManuscrypt on more than 35,000 computers in 195 countries of the world.

The graph below shows day-to-day changes in the number of computers on which PseudoManuscrypt was blocked. The two obvious surges on the graph – on March 27 and May 15 – correspond to the dates of release / distribution start of new PseudoManuscrypt versions.



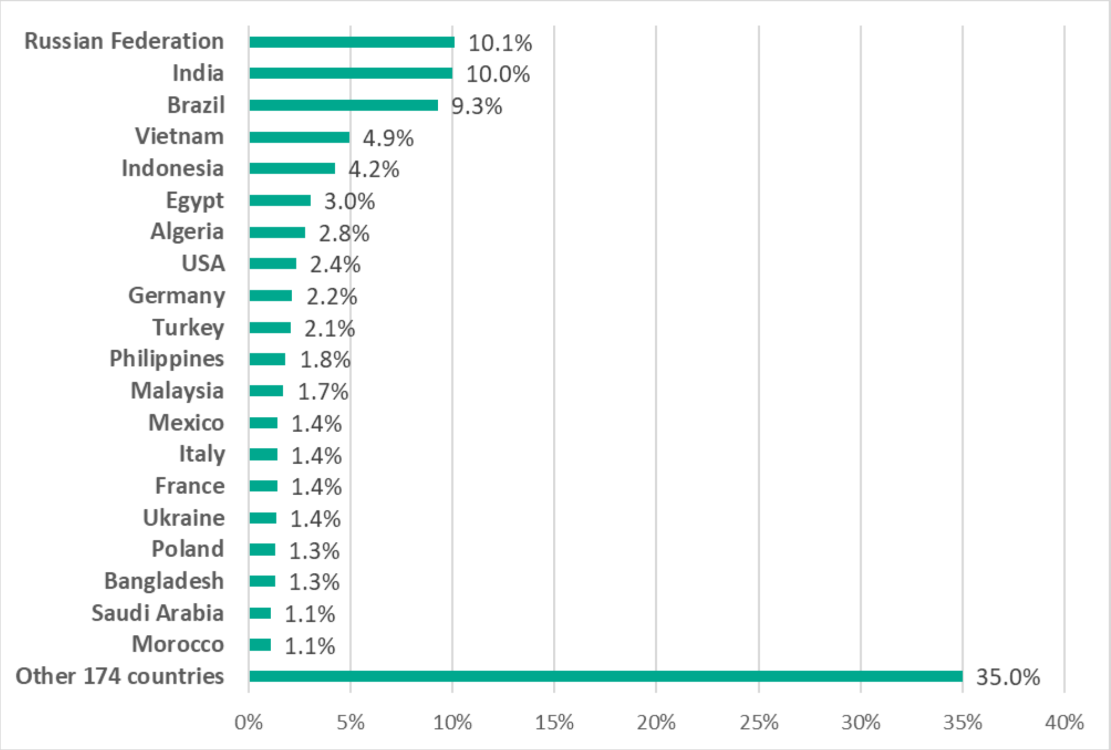
Number of systems on which PseudoManuscrypt was detected, by day

At least 7.2% of all computers on which PseudoManuscrypt was blocked are ICS computers.



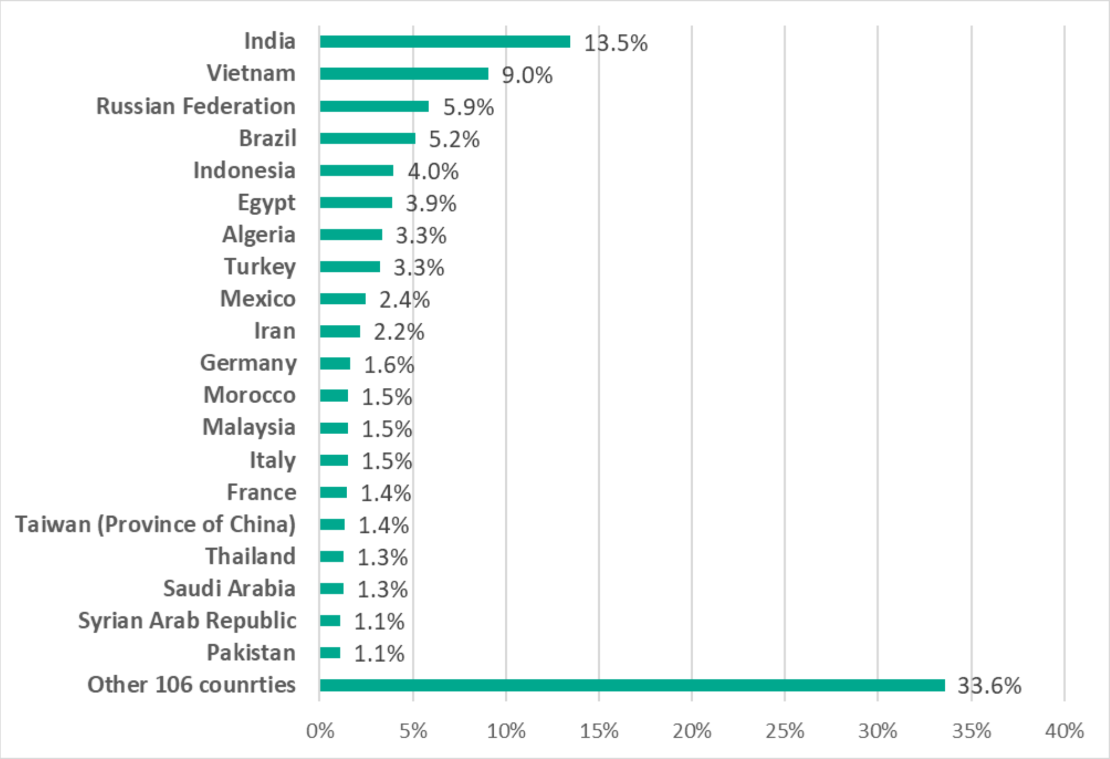
Share of industrial systems in the overall set of computers attacked by PseudoManuscrypt

As shown in the diagram below, nearly a third (29.4%) of non-ICS computers are located in Russia (10.1%), India (10%), and Brazil (9.3%).



Percentage of non-ICS computers attacked by PseudoManuscrypt in different countries

The distribution of non-ICS computers attacked by PseudoManuscrypt by country is similar to that for ICS computers. However, some countries, most of which are located in Asia and the Middle East, show significantly higher percentages (by factors of 1.5 - 2) in the country ranking for ICS computers attacked than in the country ranking for non-ICS computers attacked.

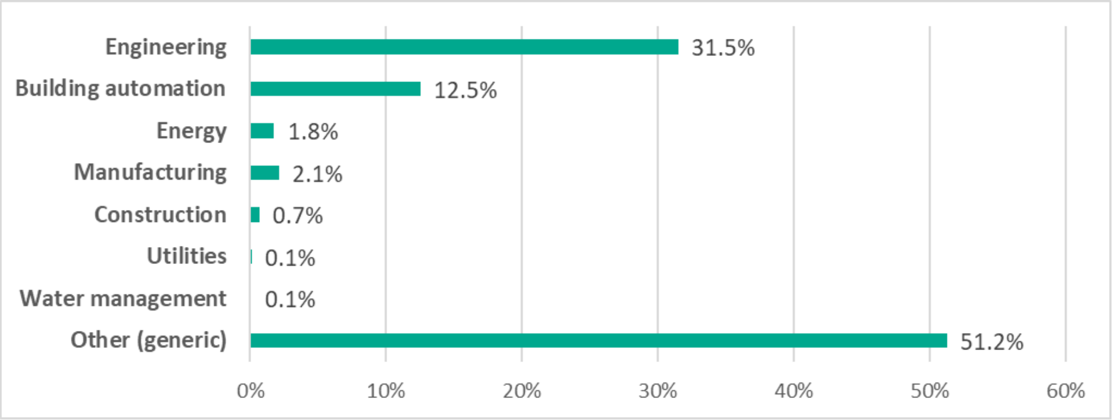


Percentage of ICS computers attacked by PseudoManuscrypt, by country

A significant proportion (31.5%) of industrial systems on which PseudoManuscrypt was blocked are apparently used for engineering, i.e., developing and launching the production of various industrial products, as well as for ICS development and integration – in different industries, including the defense and energy industries. This includes computers used for 3D modeling and physical simulations, as well as computers that have software for creating ‘digital twins’ installed on them.

In addition, about 12.5% of computers on which PseudoManuscrypt was blocked belong to building automation systems (including video surveillance, access control systems, notification systems, etc.), 1.8% in the energy sector, 2.1% in various manufacturing facilities, 0.7% in construction (structural engineering), 0.1% in public utility computers and 0.1% on computers used in water treatment systems.

About 51.2% of industrial computers on which PseudoManuscrypt was blocked are general-purpose ICS, which we cannot link to a specific industry with sufficient confidence.



Distribution of industrial systems attacked by PseudoManuscrypt by industry

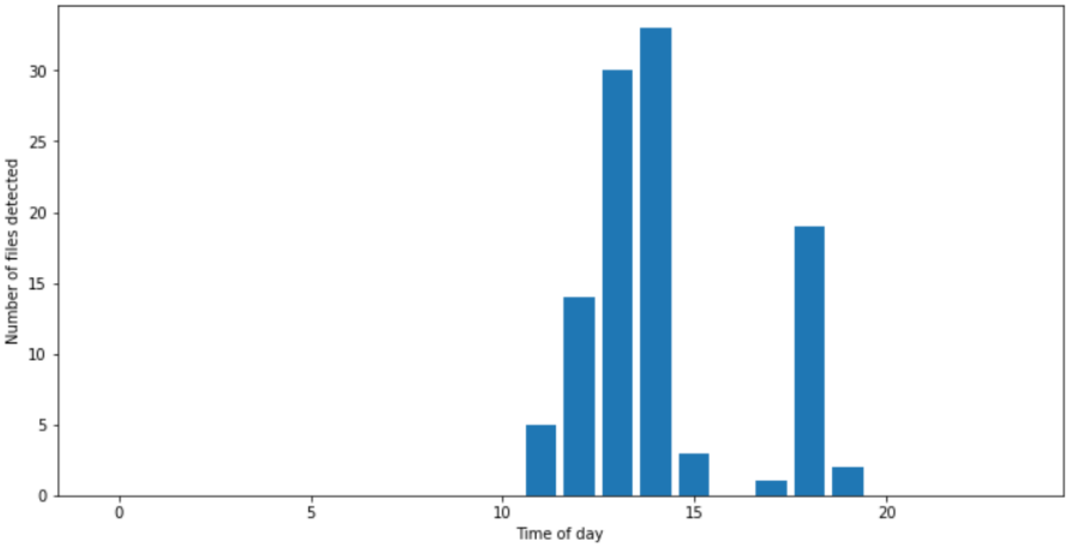
It was established in the course of the research that attack victims include, among others, enterprises connected with the military-industrial complex (such as research labs).

Another curious fact is that, judging by information from public sources, some of the organizations attacked by PseudoManuscrypt have business and production ties with organizations that fell victim to the attack described in the following Kaspersky report: "Lazarus Targets Defense Industry with ThreatNeedle".

About the attackers

A set of clues we have found may potentially point at the origin of the adversary or its ties:

1. Some malware samples contain comments in Chinese in executable file metadata.
2. Data is sent to the attackers' server using a library that has previously been used only in malware of the Chinese group APT41.
3. When connecting to the command-and-control server, the malware specifies Chinese as the preferred language.
4. The malicious file contains code for connecting to Baidu, a popular Chinese cloud storage for files.
5. The time of day at which new versions of the PseudoManuscrypt loader were uploaded by the developer falls within the 11 am to 7 pm interval in the GMT+8 time zone, in which several East Asian and Asia-Pacific countries are located.



Threat actor malware testing activity times

Conclusion

Despite collecting and analyzing a large amount of data, it seems to us that many of our findings remain unexplained and do not fit any known schemes.

Thus, we cannot say for certain whether the campaign is pursuing criminal mercenary goals or goals correlating with some governments' interests. Nevertheless, the fact that attacked systems include computers of high-profile organizations in different countries makes us assess the threat level as high.

The number of attacked systems is large and we see no clear focus on specific industrial organizations. However, the fact that a large number of ICS computers across the globe (many hundreds according to our telemetry alone – and in reality very likely to be much more) have been attacked in this campaign certainly makes it a threat that merits the very closest attention of specialists responsible for the security and safety of shop-floor systems and their continuous operation.

The large number of engineering computers attacked, including systems used for 3D and physical modeling, the development and use of digital twins raises the issue of industrial espionage as one of the possible objectives of the campaign.

We are not wrapping up our investigation as yet and will release information on new findings as they appear.

If you have any questions or comments after reading this report or if you have any additional information that is relevant to the malicious campaign described in it, please do not hesitate to get in touch with us by sending an email to ics-cert@kaspersky.com.

Recommendations

1. Install endpoint protection software on all servers and workstations, be sure to enable centralized security policy management for it (with no administration rights assigned to the end-user), and ensure that the databases and program modules of the security solution are kept up-to-date.
2. Check that all endpoint protection components are enabled on all systems and that a policy is in place which requires the administrator password to be entered in the event of attempts to disable protection.
3. Check that Active Directory policies include restrictions on user attempts to log in to systems. Users should only be allowed to log in to those systems which they need to access to perform their job responsibilities.
4. Restrict network connections, including VPN, between systems on the OT network; block connections on all those ports the use of which is not required for the continuity and safety of operations.
5. Use smart cards (tokens) or one-time codes as the second authentication factor when establishing a VPN connection. In cases where this is applicable, use the Access Control List (ACL) technology to restrict the list of IP addresses from which a VPN connection can be initiated.
6. Train employees of the enterprise in working with the internet, email and other communication channels securely and, specifically, explain the possible consequences of downloading and executing files from unverified sources.
7. Use accounts with local administrator and domain administrator privileges only when this is necessary to perform the job responsibilities.
8. Restrict the ability of programs to gain SeDebugPrivilege privileges (where possible).
9. Enforce a password policy that has password complexity requirements and requires passwords to be changed on a regular basis.
10. Consider using Managed Detection and Response class services to gain quick access to high-level knowledge and expertise of security professionals.
11. Use dedicated protection for shop-floor systems. Kaspersky Industrial CyberSecurity protects industrial endpoints and enables OT network monitoring to identify and block malicious activity.

Indicators of compromise (IOC)

Checksums (MD5)

In this section, we list MD5 hashes of those files which we believe were used in the attack but not those of test malware samples

1fecb6eb98e8ee72bb5f006dd79c6f2f

4da2c2abcf1df9749b64b34160bd3ebf

5dc7fbf2141f7dfe5215c94895bf959c

70e9416833b2f933b765042f8e1ea0bc

8074f73f7742309b033676cd03eb0928

8ae40c8418b2c36b58d2a43153544ddd

File paths

%WinDir%\System32\[0-Z]{10}.tmp e.g. I59RFRLY9J.tmp

%TEMP%\[0-Z]{10}.tmp e.g. I59RFRLY9J.tmp

%WinDir%\System32\9cda11af69ab0a2b6a9167f7131e7b93.key

Security solution verdicts

Trojan.Win64.Manuscrypt.do

URL addresses

hxxp://email.yg9[.]me

hxxp://google.vrthcobj[.]com

hxxp://d.diragame[.]com

toa.mygametoa[.]com

tob.mygametob[.]com

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global project of Kaspersky aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT

ics-cert@kaspersky.com