LuckyMouse signs malicious NDISProxy driver with certificate of Chinese IT company

securelist.com/luckymouse-ndisproxy-driver/87914

By GReAT

What happened?

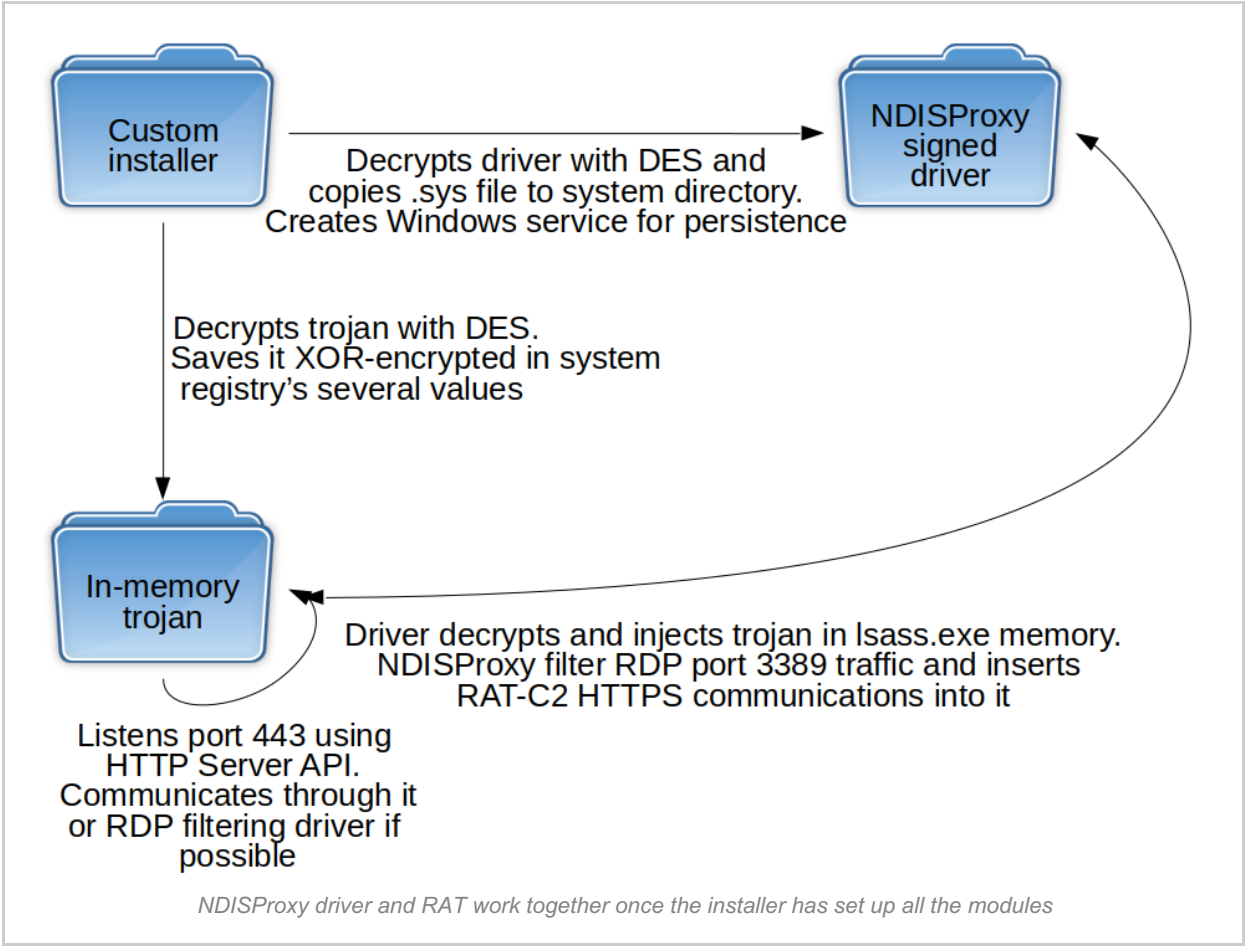
Since March 2018 we have discovered several infections where a previously unknown Trojan was injected into the lsass.exe system process memory. These implants were injected by the digitally signed 32- and 64-bit network filtering driver NDISProxy. Interestingly, this driver is signed with a digital certificate that belongs to Chinese company LeagSoft, a developer of information security software based in Shenzhen, Guangdong. We informed the company about the issue via CN-CERT.

The campaign described in this report was active immediately prior to Central Asian high-level meeting and we suppose that actor behind still follows regional political agenda.

Which malicious modules are used?

The malware consists of three different modules:

- A custom C++ installer that decrypts and drops the driver file in the corresponding system directory, creates a Windows autorun service for driver persistence and adds the encrypted in-memory Trojan to the system registry.
- A network filtering driver (NDISProxy) that decrypts and injects the Trojan into memory and filters port 3389 (Remote Desktop Protocol, RDP) traffic in order to insert the Trojan's C2 communications into it.
- A last-stage C++ Trojan acting as HTTPS server that works together with the driver. It waits passively for communications from its C2, with two possible communication channels via ports 3389 and 443.



NDISProxy driver and RAT work together once the installer has set up all the modules

These modules allow attackers to silently move laterally in the infected infrastructure, but don't allow them to communicate with an external C2 if the new infected host only has a LAN IP. Because of this, the operators used an Earthworm SOCKS tunneler in order to connect the LAN of the infected host to the external C2. They also used the Scanline network scanner to find file shares (port 135, Server Message Block, SMB) which they use to spread malware with administrative passwords, compromised with keyloggers.

We assess with high confidence that NDISProxy is a new tool used by LuckyMouse. Kaspersky Lab products detect the described artefacts. For more information please contact: intelreports@kaspersky.com

How does it spread?

We detected the distribution of the 32-bit dropper used for this campaign among different targets by the end of March 2018. However, we didn't observe any spear phishing or watering hole activity. We believe the operators spread their infectors through networks that were already compromised instead.

How does it work?

Custom installer

Installer MD5 hash	Timestamp (GMT)	Size	Bits
dacedff98035f80711c61bc47e83b61d	2018.03.29 07:35:55	572 244	32

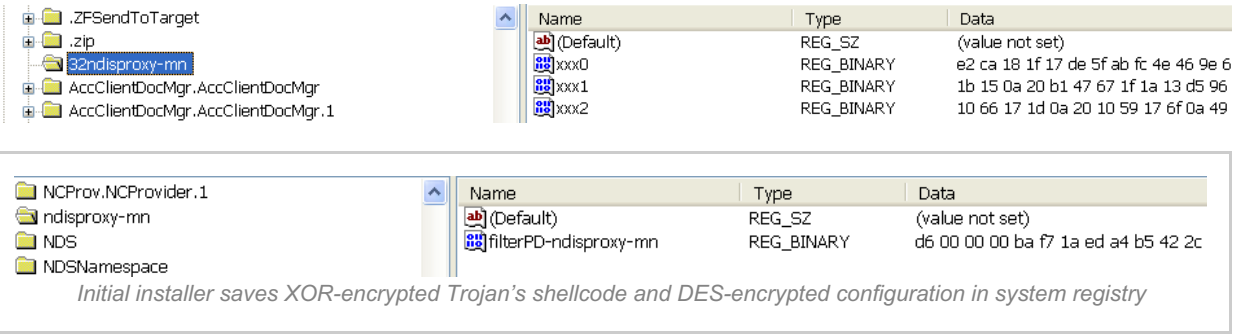
9dc209f66da77858e362e624d0be86b3	2018.03.26 04:16:00	572 244	32
3cbeda2c5ac41cca0b0d60376a2b2511	2018.03.26 04:16:00	307 200	32

The initial infectors are 32-bit portable executable files capable of installing 32-bit or 64-bit drivers depending on the target. The installer logs all the installation process steps in the load.log file within the same directory. It checks if the OS is Windows Vista or above (major version equal to 6 or higher) and decrypts its initial configuration using the DES (Data Encryption Standard) algorithm.

The set of well-known port numbers (HTTP, HTTPS, SMB, POP3S, MSSQL, PPTP and RDP) in the configuration is not used, which along with the “[test]” strings in messages suggests this malware is still under development.

The installer creates a semaphore (name depending on configuration) Global\Door-ndisproxy-mn and checks if the service (name also depends on configuration) ndisproxy-mn is already installed. If it is, the dropper writes “door detected” in load.log. The autorun Windows service running NDISProxy is the “door” in developer terms.

The installer also decrypts (using the same DES) the shellcode of the last stage Trojan and saves it in three registry values named xxx0, xxx1, xxx2 in key HKLM\SOFTWARE\Classes\32ndisproxy-mn (or 64ndisproxy-mn for 64-bit hosts). The encrypted configuration is saved as the value filterpd-ndisproxy-mn in the registry key HKCR\ndisproxy-mn.



Initial installer saves XOR-encrypted Trojan’s shellcode and DES-encrypted configuration in system registry

The installer creates the corresponding autostart service and registry keys. The “Altitude” registry value (unique ID for the minifilter driver) is set to 321 000, which means “FSFilter Anti-Virus” in Windows terms:

FSFilter Anti-Virus	320000-329999	This group includes filter drivers that detect and disinfect viruses during file I/O.

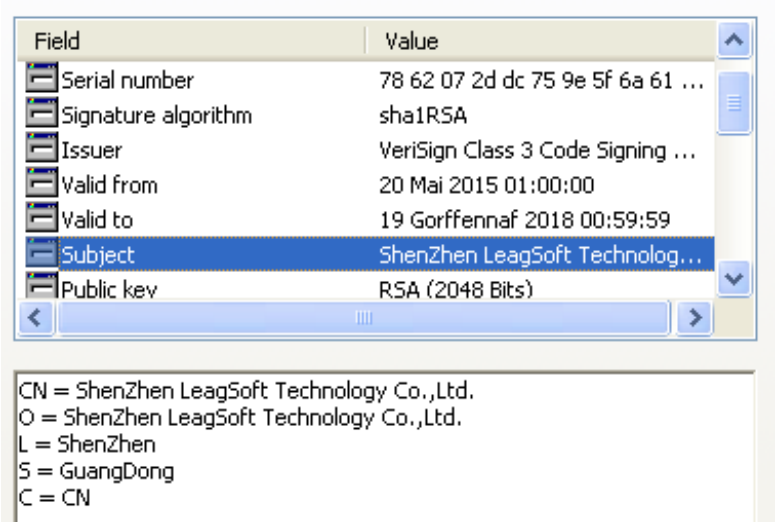
NDISProxy network filtering driver

Driver MD5 hash	Timestamp	Size	Bits
8e6d87eadb27b74852bd5a19062e52ed	2018.03.29 07:33:58	40400	64
d21de00f981bb6b5094f9c3dfa0be533	2018.03.29 07:33:52	33744	32
a2eb59414823ae00d53ca05272168006	2018.03.26 04:15:28	40400	64

493167e85e45363d09495d0841c30648	2018.03.26 04:15:21	33744	32
ad07b44578fa47e7de0df42a8b7f8d2d	2017.11.08 08:04:50	241616	64

This digitally signed driver is the most interesting artefact used in this campaign. The network filtering modules serve two purposes: first they decrypt and inject the RAT; second, they set its communication channel through RDP port 3389.

The drivers are signed with a digital certificate issued by VeriSign to LeagSoft, a company developing information security software such as data loss prevention (DLP) solutions.



This driver makes extensive use of third-party publicly available C source code, including from the Blackbone repository available at GitHub.

Feature	Public repository
Driver memory injection	Blackbone https://github.com/DarthTon/Blackbone
NDIS network filtering driver	Microsoft Windows Driver Kit (WDK) sample code “Windows Filtering Platform Stream Edit Sample/C++/sys/stream_callout.c”
Parse HTTP packets	Http-parser https://github.com/nodejs/http-parser

The driver again checks if the Windows version is higher than Vista, then creates a device named \\Device\\ndisproxy-%s (where the word after “-” varies – see Appendix for all variants) and its corresponding symbolic link \\DosDevices\\Global\\ndisproxy-%s.

The driver combines all the Trojan-related registry values from HKLM\SOFTWARE\Classes\32ndisproxy-mn and de-XORs them with a six-byte hardcoded value. It then injects the resulting Trojan executable shellcode into lsass.exe memory using Blackbone library functions.

NDISProxy works as a network traffic filter engine, filtering the traffic going through RDP port 3389 (the port number is hardcoded) and injecting messages into it.

The communication between the user-mode in-memory Trojan and the driver goes through the custom control codes used by the DeviceIoControl() Windows API function. Apart from the auxiliary codes, there are two codes worth mentioning:

Driver control code	Meaning
0x222400	Start traffic filtering at RDP port 3389
0x22240C	Inject given data into filtering TCP stream. Used for Trojan communication with C2

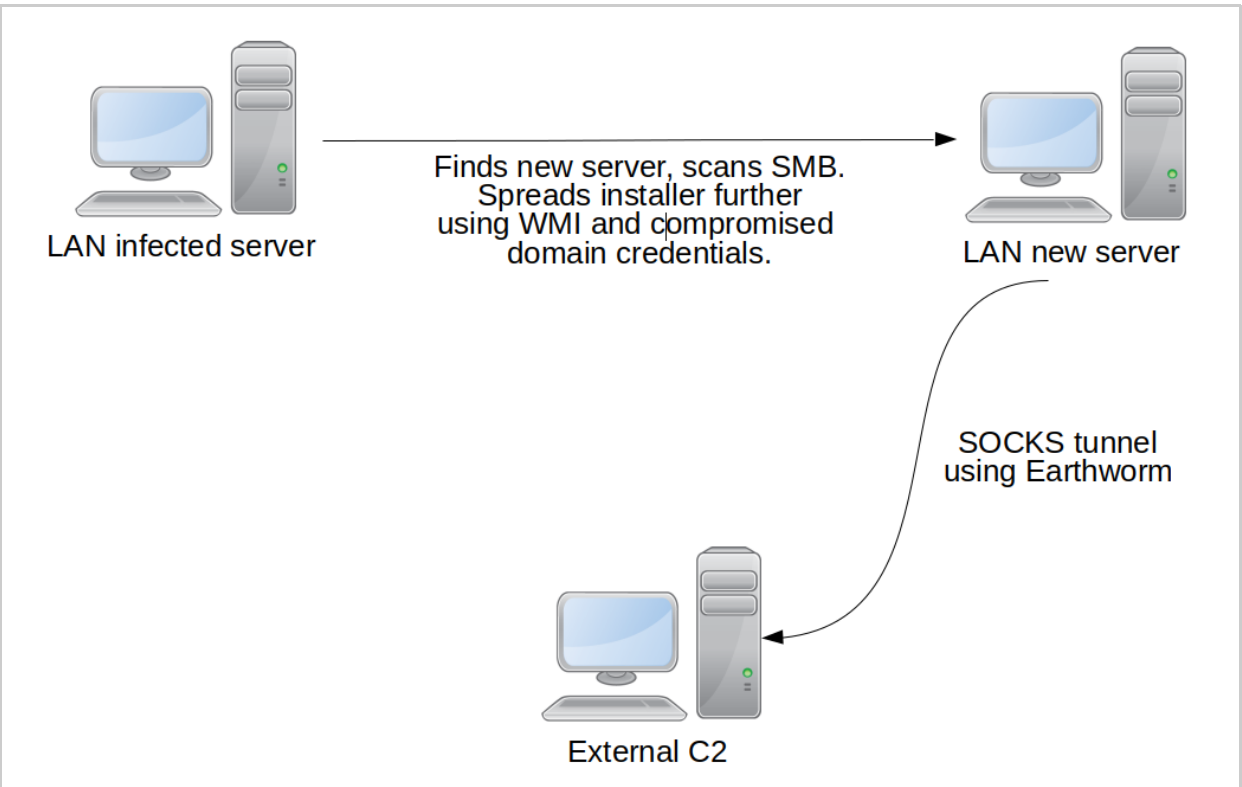
In-memory C++ Trojan

SHA256	c69121a994ea8ff188510f41890208625710870af9a06b005db817934b517bc1
MD5	6a352c3e55e8ae5ed39dc1be7fb964b1
Compiled	2018.03.26 04:15:48 (GMT)
Type	I386 Windows GUI DLL
Size	175 616

Please note this Trojan exists in memory only; the data above is for the decrypted Windows registry content without the initial shellcode

This RAT is decrypted by the NDISProxy driver from the system registry and injected into the lsass.exe process memory. Code starts with a shellcode – instead of typical Windows portable executable files loader this malware implements memory mapping by itself.

This Trojan is a full-featured RAT capable of executing common tasks such as command execution and downloading/uploading files. This is implemented through a couple dozen C++ classes such as CMFile, CMFile, CMProcess, TFileDownload, TDrive, TProcessInfo, TSock, etc. The first stage custom installer utilizes the same classes. The Trojan uses HTTP Server API to filter HTTPS packets at port 443 and parse commands.



The Trojan is an HTTP server, allowing LAN connection. It uses a SOCKS tunneler to communicate with the C2

This Trojan is used by attackers to gather a target's data, make lateral movements and create SOCKS tunnels to their C2 using the Earthworm tunneler. This tool is publicly available and popular among Chinese-speaking actors. Given that the Trojan is an HTTPS server itself, we believe that the SOCKS tunnel is used for targets without an external IP, so the C2 is able to send commands.

Who's behind it and why?

We found that this campaign targeted Middle Asian governments' entities. We believe the attack was highly targeted and was linked to a high-level meeting. We assess with high confidence that the Chinese-speaking LuckyMouse actor is responsible for this new campaign using the NDISProxy tool described in this report.

In particular, the choice of the Earthworm tunneler is typical for Chinese-speaking actors. Also, one of the commands used by the attackers ("-s rssocks -d 103.75.190[.]28 -e 443") creates a tunnel to a previously known LuckyMouse C2. The choice of victims in this campaign also aligns with the previous interests shown by this actor.

Consistent with current trends

We have observed a gradual shift in several Chinese-speaking campaigns towards a combination of publicly available tools (such as Metasploit or CobaltStrike) and custom malware (like the C++ last stage RAT described in this report). We have also observed how different actors adopt code from GitHub repositories on a regular basis. All this combines to make attribution more difficult.

This campaign appears to demonstrate once again LuckyMouse's interest in Central Asia and the political agenda surrounding the Shanghai Cooperation Organization.

Indicators of Compromise

Note: *The indicators in this section are valid at the time of publication. Any future changes will be updated directly in the corresponding .ioc file.*

File Hashes

Droppers-installers
9dc209f66da77858e362e624d0be86b3
dacedff98035f80711c61bc47e83b61d

Drivers
8e6d87eadb27b74852bd5a19062e52ed
d21de00f981bb6b5094f9c3dfa0be533
a2eb59414823ae00d53ca05272168006
493167e85e45363d09495d0841c30648
ad07b44578fa47e7de0df42a8b7f8d2d

Auxiliary Earthworm SOCKS tunneler and Scanline network scanner
83c5ff660f2900677e537f9500579965

3a97d9b6f17754dcd38ca7fc89caab04

Domains and IPs

103.75.190[.]28
213.109.87[.]58

Semaphores

Global\Door-ndisproxy-mn
Global\Door-ndisproxy-help
Global\Door-ndisproxy-notify

Services

ndisproxy-mn
ndisproxy-help
ndisproxy-notify

Registry keys and values

HKLM\SOFTWARE\Classes\32ndisproxy-mn
HKLM\SOFTWARE\Classes\64ndisproxy-mn
HKCR\ndisproxy-mn\filterpd-ndisproxy-mn
HKLM\SOFTWARE\Classes\32ndisproxy-help
HKLM\SOFTWARE\Classes\64ndisproxy-help
HKCR\ndisproxy-mn\filterpd-ndisproxy-help
HKLM\SOFTWARE\Classes\32ndisproxy-notify
HKLM\SOFTWARE\Classes\64ndisproxy-notify
HKCR\ndisproxy-mn\filterpd-ndisproxy-notify

Driver certificate

A lot of legitimate LeagSoft products are signed with the following certificate. Please don’t consider all signed files as malicious.

Subject	ShenZhen LeagSoft Technology Co.,Ltd.
Serial number	78 62 07 2d dc 75 9e 5f 6a 61 4b e9 b9 3b d5 21
Issuer	VeriSign Class 3 Code Signing 2010 CA
Valid to	2018-07-19