← Blog

Sharmine Low

Malware Analyst, APAC

Curse of the Krasue: New Linux Remote Access Trojan targets Thailand

This piece of malware has an insatiable appetite. Group-IB's Threat Intelligence unit offers their insights on the new RAT used in attacks against Thai companies.

December 7, 2023 · min to read · Malware Analysis

Krasue Thailand Trojan

The appetite of cybercriminals is insatiable. With increasing regularity, we are seeing the proliferation of new schemes, groups, and malware all designed to wreak havoc and destruction. Earlier this year, the Group-IB Threat Intelligence unit uncovered a **Linux Remote Access Trojan (RAT)** that has managed to fly under the radar for a long time. Group-IB researchers discovered that this malware, which was first registered on Virustotal in **2021**, has almost exclusively been used against organizations in Thailand. At the time of writing, Group-IB researchers can confirm that Krasue was used against **telecommunications companies**, although it has likely been leveraged in attacks against organizations in other verticals as well.

Owing to the fact that Thai companies were exclusively targeted, Group-IB has decided to call this RAT **Krasue**, a nod to the Thai name of a nocturnal native spirit known throughout Southeast Asian folklore. Krasue, who is said to hover in the air above the ground and is driven by extreme hunger, poses a severe risk to critical systems and sensitive data given that it is able to grant attackers remote access to the targeted network. The malware also features rootkits embedded in the binary.

In this article, we explore **Krasue's key characteristics**, shedding light on its functionalities, potential impact, and the measures that organizations should take to defend against the evolving threat. Krasue's core functionality lies in its ability to **maintain access to the host**, hence we presume that it is either **deployed as part of a botnet** or **sold by initial access brokers** to other cybercriminals who are looking to acquire access to a particular target. The information contained in this blog post is useful for organizations fighting cybercrime and technical specialists – intelligence analysts, incident responders and malware analysts.

Key takeaways

Krasue is a **Linux Remote Access Trojan** that has been active since 2021 and predominantly targets organizations in **Thailand.**

Group-IB can confirm that **telecommunications** companies were targeted by Krasue.

The malware contains **several embedded rootkits** to support different Linux kernel versions.

Krasue's rootkit is drawn from public sources (3 open-source Linux Kernel Module rootkits), as is the case with many Linux rootkits.

The rootkit can hook the **`kill()` syscall**, network-related functions, and file listing operations in order to **hide its activities and evade detection.**

Notably, Krasue uses **RTSP (Real-Time Streaming Protocol)** messages to serve as a disguised "alive ping," a tactic **rarely seen in the wild.**

This Linux malware, Group-IB researchers presume, is deployed during the **later stages of an attack chain** in order to maintain access to a victim host.

Krasue is likely to either be deployed as part of a botnet or sold by initial access brokers to other cybercriminals.

Group-IB researchers believe that Krasue was created by the same author as the **XorDdos Linux Trojan**, documented by Microsoft in a March 2022 blog post, or someone that had access to the latter's source code.

During the initialization phase, the rootkit conceals its own presence. It then proceeds to hook the **`kill()`** syscall, network-related functions and file listing operations, thereby obscuring its activities and evading detection.

Krasue feeds at night

To date, the malware named Krasue by Group-IB experts has not been publicly described. Group-IB researchers have not yet determined Krasue's initial infection vector and the scale of its usage. Several potential pathways by which Krasue could enter a system include **vulnerability exploitation**, **credential brute force attacks**, and, more uncommonly, being **unwittingly downloaded as part of a deceptive package or binary** (i.e. a file masquerading as a product update) from an untrustworthy third-party source.

Group-IB can confirm that **telecommunications companies in Thailand** were targeted with Krasue, and that it is likely that this RAT is used later in the attack chain, once a cybercriminal has already intruded into the target network.

Figure 1. Krasue profile made by Group-IB Threat Intelligence.

Group-IB Threat Intelligence researchers wished to make their derived unique insights into this malware known to the public at this stage, so that **organizations in Thailand can take steps to protect themselves,** and that the global cybersecurity community can better understand the evolving functionalities of Linux RATs and hunt for them. As a result, we have included **a full list of YARA rules** at the end of this blog, and Group-IB will share any updates regarding this threat on our public platforms. Additionally, in line with the company's zero-tolerance policy to cybercrime, **Group-IB's Computer Emergency Response Team** (GIB-CERT) shared our findings into Krasue with the **Thailand Computer Emergency Response Team (ThaiCERT)** and the **Thailand Telecommunications Sector Computer Emergency Response Team (TTC-CERT)**.

So why has Krasue flown under the radar? Firstly, older Linux servers often have poor **Endpoint Detection & Response (EDR) coverage**. Secondly, packed malware samples typically are more difficult to detect by security solutions. Specifically, this malware uses **UPX packing**, and it also enhances its evasion capabilities by daemonizing itself, running as a background process, and disregarding **SIGINT** signals. By ignoring SIGINT signals, the process remains unaffected by interrupt signals sent when the user terminates the process by pressing Ctrl-C. If the program has root privileges, it proceeds to install a rootkit (more details in the next section).

Krasue creates a child process and establishes a **UDP socket server** on port 52699. The purpose of this server is to wait for commands from a command and control (C2) server. For C2 communication, the traffic undergoes AES-CBC encryption using a static key: `**22 32 A4 98 A1 4F 2E 44 CF 55 93 B7 91 59 BE A6**`. The author used the tiny-AES library. The Trojan handles C2 commands as shown below:

C2 command	Description
ping	Reply with `pong`
master	Set the master upstream C2
info	Get information about the malware: main pid, child pid, and its status such as root: gained root permissions god: process is unable to be killed hidden: process is hidden module: rootkit is loaded
restart	Restart child process
respawn	Restart main process
god die	Kill itself
shell	Run shell commands with `/bin/sh`

Krasue is able to designate a communicating IP as its master C2. It constantly sends `**DESCRIBE rtsp://server/media[.]mp4 RTSP/1.0\r\nCSeq: 2\r\n\r\n**` in the form of an alive ping to its master C2, in which it returns a blank space character `**\x20**`. `DESCRIBE` is a method used in **Real Time Streaming Protocol (RTSP)**, a network protocol designed for controlling the delivery of real-time media streams over IP networks. It is often used in applications such as video streaming and video surveillance systems.

We found a total of **9 hardcoded IP addresses** for its master C2. Krasue will always attempt to connect to the internal addresses initially. Only after multiple non-replies and trying to connect to server after server, it will attempt to connect **128[.]199[.]226[.]11** at port **554**, which is a port commonly used for RTSP. We suspect that the program is attempting to masquerade and camouflage its network communication, and this is notable because while malware developers typically make a concerted effort to disguise network traffic, **using RTSP for this purpose is highly uncommon**.

There are two possible reasons why Krasue has multiple (8) internal IP addresses contained within it. The first is that the internal IP addresses are deliberately fabricated to mislead sandbox analyses and only connect to the external IPs after running for a certain period of time.

The second possibility is that the cybercriminals had access to the Remote Access Trojan from within the victim's infrastructure since the malware does not have reverse proxy capabilities. The hackers may have gained access to the victim's infrastructure and created tunnels within the

network. This would also suggest that Krasue is typically deployed during the later stages of an attack chain in order to maintain remote access to an infected network.

- 172[.]19[.]37[.]145: 52699
- 172[.]19[.]37[.]159: 52699
- 172[.]19[.]37[.]169: 52699
- 172[.]19[.]37[.]170: 52699
- 172[.]19[.]37[.]171: 52699
- 172[.]19[.]37[.]172: 52699
- 172[.]19[.]37[.]173: 52699
- 172[.]19[.]37[.]175: 52699
- 128[.]199[.]226[.]11: 554

The only external master C2 IP address of the analyzed sample is **128.199.226[.]11**.

Analysis of Krasue.Rootkit

The Krasue rootkit is a **Linux Kernel Module** (LKM) and targets Linux Kernel versions **2.6x/3.10.x.** An LKM is an object file that can be dynamically loaded into the Linux kernel at runtime. It extends the functionality of the kernel without having to recompile or modify the entire kernel source code. The rootkit masquerades as a **VMware driver** and does not contain a valid digital signature.

In order to support different Linux kernel versions, the **malware embeds 7 compiled versions of the rootkit**. After the RAT determines the kernel version by reading `**/proc/version**`, it tries to install the rootkit using the `init_module` function, which loads the ELF image into kernel space. Such modules do not persist when the system is rebooted, which is why we believe that the cybercriminals who eventually leverage Krasue gain persistence in the targeted network earlier in the attack chain.

The code seems to be based on 3 different open-source LKM rootkits:

- Diamorphine
- Suterusu
- Rooty

The embedded 7 rootkits are compiled from the same source and have the same functionalities. The hashes of the extracted rootkits can be found in the IOC section below. All the rootkits have the same fake metadata, namely the description of "**VMware User Mode Helper**".

Figure 2. Rootkit modinfo section

Stealth mechanisms

The rootkit uses **system call hooking** (by overwriting function pointers in the system call table) and **function call hooking** (by modifying the prologue of the target function).

During the initialization phase, the rootkit conceals its own presence. It then proceeds to hook the **`kill()`** syscall, network-related functions and file listing operations, thereby obscuring its activities and evading detection. Files and directories beginning with the names "**auwd**" and "**vmware_helper**" are hidden from directory listings. Furthermore, the rootkit enhances its stealth capabilities by hiding ports **52695** to **52699**.

Communication with the rootkit

The rootkit portion overlaps in a unique way with the rootkit of XorDdos, another Linux malware. The Krasue kernel rootkit has the following functions:

- Hide files and directories related to the malware
- Hide the rootkit
- Provide root access
- Hide ports and processes

There are multiple similarities between the rootkits of Krasue and **XorDdos**, another Linux malware. However, unlike XorDdos, Krasue uses **signals** instead of **`ioctl()`** to communicate with the rootkit.

Also, by intercepting the `**kill()**` syscall, kill signals issued to the malware process are conveniently ignored.

Commands can be issued to the rootkit using `**kill(arg1,signal)**` or `**kill -signal arg1**` on the terminal. Other signals that are not targeted by the rootkit will be passed to the regular `**kill()**` system call. The author used certain magic numbers like 52698, 758.

arg1	signal	Description
x	31	Make process x invisible
x	61	Unhide port x
x	62	Hide port x
52698	63	Hide/show kernel module
52698	64	Provide root privilege
758	64	Check if rootkit is loaded. Return 0xBD if loaded
x	64	Set the god pid (main pid) to x. To set the god pid, it is necessary to issue the kill command for x = 5,2,6,9,8 consecutively before finally specifying the pid.

Key similarities and differences between rootkits

The functionalities of Krasue and XorDdos are vastly different, but the components of their rootkits showed some overlaps. Linux rootkits usually do show some similarities as they take reference from public sources, but these two samples exhibit certain code portions that are pretty distinctive. Our comparison of Krasue and XorDdos rootkits was based on information taken from Microsoft's blog post detailing XorDdos and the sample (SHA256: C8F761D3EF7CD16EBE41042A0DAF901C2FDFFCE96C8E9E1FA0D422C6E31332EA) included in the IOC section of the aforementioned blog.

XorDdos.Rootkit	Krasue.Rootkit
Magic number: 62598	Magic number: 52698
`unhide_allz()` unhides all hidden TCP and UDP ports	`unhide_allz()` unhides only hidden UDP ports
Ports hidden during initialization: TCP/UDP 62595-62599 and UDP 21,22,10050	Ports hidden during initialization: TCP/UDP 52695-52699
Able to change firewall entries*	–
Maintain a hidden processes list*	–
Similarities: High code similarity Unique symbol names: unhide_allz, _kkill	

* Functionalities mentioned in Microsoft's blog post and found in other XorDdos.Rootkit samples but not found in this particular sample.

Conclusion

While the primary components of the Krasue Remote Access Trojan differ from XorDdos, there are substantial and unique overlaps in the rootkit segment. As a result, Group-IB researchers can assert with a moderate degree of confidence that Krasue was likely created by the same author as XorDdos, or by someone with access to the latter's source code.

Given that various threat actors have used code snippets from the three different open-source projects (Diamorphine, Suterusu, Rooty) to create Krasue's rootkit, it is difficult to accurately attribute the source code to a specific threat group.

The information available is not enough to put forward a conclusive attribution as to the creator of Krasue, or the groups that are leveraging it in the wild, but the fact that these malicious programs are able to remain under the radar for extended periods makes it clear that continuous vigilance

and better security measures are necessary. We will continue to monitor for future Krasue activity, especially if the RAT expands to other geographies.

Recommendations for security professionals

Use Group-IB's Threat Intelligence to obtain up-to-date information about the spread of Krasue and any updates to the Trojan.

Be on the look out for anomalous RTSP traffic.

Trustworthy sources: Download software and packages only from trusted and official sources. Stick to reputable repositories provided by your Linux distribution or verified third-party sources with a strong reputation for security.

Enable kernel module signature verification: Configure your kernel to only load signed modules. This ensures that only modules with a valid digital signature from a trusted source can be loaded.

Monitor system and network logs: Regularly review system and network logs for any suspicious activities.

Conduct periodic security audits: Perform regular security audits of your server environment. This includes reviewing system configurations, conducting vulnerability assessments, and performing penetration testing to identify any potential weaknesses and appropriate remedial actions.

Join the Group-IB Cybercrime Fighters Club!

The global fight against cybercrime is a collaborative effort, and that's why we're looking to partner with industry peers to research emerging threats and publish joint findings on our blog. If you've discovered a breakthrough into a particular threat actor or a vulnerability in a piece of software, let us know, and we can mobilize all our necessary resources to dive deeper into the issue.

All contributions will be given appropriate credit along with the full backing of our social media team on Group-IB's Threat Intelligence Twitter page, where we regularly

share our latest findings into threat actors' TTPs and infrastructure, along with our other social media accounts.

#LetsStopCybercrime #CybercrimeFightersClub

Join us now

MITRE ATT&CK®

IOCs

YARA Rules

```
rule linux_trojan_unpacked_krasue {
  meta:
        author = "Sharmine Low"
        company = "Group-IB"
        description = "Detects unpacked linux trojan krasue"
        sample = "902013bc59be545fb70407e8883717453fb423a7a7209e119f112ff6771e44cc"

  strings:
        $s1 = "DESCRIBE rtsp://server/media.mp4 RTSP/1.0"
        $s2 = "%s: main/child pid: %d/%d root/god/hidden/module"
        $s3 = "god die"
        $s4 = "set master done"

  condition:
        2 of ($s*)
}

rule linux_rootkit_krasue {

  meta:
        author = "Sharmine Low"
        company = "Group-IB"
```

```
        description = "Detects krasue kernel rootkit, overlaps with xorddos rootkit"
        sample = "3e37c7b65c1e46b2eb132f98f65c711b4169c6caeeaecc799abbda122c0c4a59"

    strings:
        $s1 = "unhide_allz"
        $s2 = "kkill"
        $s3 = "is_invisible"
        $s4 = "give_root"
        $s5 = "hide_tcp4_port"

    condition:
        4 of them
}
```


Contact

APAC: +65 3159 3798

EU & NA: +31 20 226 90 90

MEA: +971 4 568 1785

info@group-ib.com

Subscribe to stay up to date with the latest cyber threat trends