

LimeRat Malware: Delivery Techniques and Organizational Impact

 cyberint.com/blog/dark-web/limerat-malware-delivery-techniques-and-organizational-impact

Adi Bleih

July 12, 2026

Dark Web

Introduction to LimeRat Malware

Lime RAT stands out as an openly available and meticulously documented malware suite built on the .NET framework, boasting a multitude of capabilities that can be highly destructive when wielded proficiently. Its capacity to pilfer a wide array of valuable data, employ encryption for ransom purposes, or transform the targeted host into a basic-capability bot, combined with an easy-to-use control panel interface, positions it as a preferred choice for less experienced operators.

With features such as anti-virus evasion, anti-virtual machine mechanisms, a minimal system footprint, and encrypted communication, Lime RAT holds appeal for threat actors spanning the entire skill spectrum. To safeguard against multifaceted threats like Lime RAT infiltrating a system through phishing campaigns, the primary approach is to educate end-users about the risks associated with suspicious emails and attachments.

Delivery Methods of LimeRat Malware

The Microsoft Office is one of the most popular tools, its popularity was abused by cybercriminals to deliver malware. In 2020, Threat actors managed a malicious campaign where they used to deliver the LimeRAT within Excel file with password-protected, to open the file victims should enter the password and it is included in the social engineered email.

LimeRAT malware is predominantly disseminated through various means, including email attachments, malicious online advertisements, social engineering tactics, and downloadable software “cracks.”

Impact of LimeRat Malware

What sets LimeRAT apart is its versatility in carrying out a multitude of malicious actions. These encompass activities such as keylogging, password theft, and screen capture. Moreover, LimeRAT is capable of executing arbitrary commands, transferring files both to and from the compromised system, and can even employ the infected machine for cryptocurrency mining or launching DDoS attacks.

About Check Point Exposure Management

Check Point Exposure Management is an intelligence-led, validation-driven, remediation-first unified platform that helps security teams move quickly and safely from exposure visibility to exposure reduction. Delivered through a single UI, it brings together threat intelligence, exposure prioritization, Agentic Exposure Validation, and safe remediation so teams can understand risk, prove exploitability, and act from one place.

[Schedule Your Demo Now](#)

LimeRat Malware TTPS

Tactic Name	Technique
Defense Evasion	T1027 – Obfuscated Files or Information
Reconnaissance	T1590 – Gather Victim Network Information
Initial Access	T1199 – Trusted Relationship
Initial Access	T1189 – Drive-by Compromise
Initial Access	T1195 – Supply Chain Compromise
Initial Access	T1456 – Drive-By Compromise
Reconnaissance	T1592 – Gather Victim Host Information
Initial Access	T1190 – Exploit Public-Facing Application
Lateral Movement	T0859 – Valid Accounts
Persistence	T0859 – Valid Accounts
Initial Access	T0817 – Drive-by Compromise
Initial Access	T0862 – Supply Chain Compromise
Reconnaissance	T1591 – Gather Victim Org Information
Initial Access	T1566 – Phishing
Initial Access	T0819 – Exploit Public-Facing Application
Initial Access	T1474 – Supply Chain Compromise
Persistence	T1078 – Valid Accounts
Initial Access	T1078 – Valid Accounts
Privilege Escalation	T1078 – Valid Accounts
Defense Evasion	T1078 – Valid Accounts

LimeRat Malware IOCs (Sample of 50)

Type	Date Added	Value
SHA-256	2026-05-29	b29cf2fc83f2c5871baf6d54b9593dec38a09208818482ec5f94947745ca7f11

Type	Date Added	Value
SHA-256	2026-05-16	940e18e109ff6af1d6c8ab01f00746034ae67dd62c49a2353931b91ef36f4e0d
SHA-256	2026-04-29	f5f67f6e64c6524f7cd1dcda342b95c9c175f86e7e2c10c24dd5af478f0a0b40
URL	2025-09-30	http://14.184.40.239:9800/Du%20lieu/DL%20A%20Tuyen/TAI%20LIEU%20CHUNG/client/Expllorer.exe
MD5	2025-09-30	96adc2ba45dff4d5d37bba5aebca86f
SHA-1	2025-09-30	704c056858e72bece27aea03d81dea070a239b6a
SHA-256	2025-09-28	edd435f7c653f3fc19e95b5a088f30476bac4fea1b63333902e1ec2eed6b7499
SHA-256	2025-06-22	81fb9aba4bee634b3a5ae80a974416d713c7e99e226be813c07e3850a92d4d99
SHA-256	2025-06-06	618f5e23d3c910b509f9032fb8ef105a1b9774598f6e0409fbef044f45204cf9
URL	2025-06-04	https://raw.githubusercontent.com/ducminh23/ducminh23/main/New-Client.exe
SHA-256	2025-05-03	236f4ff5a788811a7de51b80e293c2203f8c2dc43a602560527f054653638606
SHA-256	2025-05-02	ba870136fc03dee7dd8df18b7e5ddf7e6a67bff8da174f0e89893aae83dc48ca
SHA1	2024-07-19	d81c0e03872d9c843087492ca1dc51572454662b
MD5	2024-07-19	363c0e3637bc0f5bf21ff253d8ab3413
SHA256	2024-07-19	0794bc31d71174be2e372f0166e041f1a6653d63df29f9aebf19233e477ea9b2
SHA256	2024-06-09	c9101aac915418735b74d5120cae0cdef803555d9a8399cf9ee5457d5c790513
SHA256	2024-06-08	ceca4ad3a264bb47c499b1fd9ac2d89e70ecda197164742be6e3c57d30a3bde7

Type	Date Added	Value
URL	2024-05-23	https://pastebin.com/raw/6bPeUTd1
SHA256	2024-05-23	a7b1c2a715bb2f2a6358825f341bcd9e3db00164f44afae1a1e8538ebfdf3a9f
SHA1	2024-05-11	b117999cc232f0faf9ff619dcabe34cea1f4d37e
SHA256	2024-05-11	93a09a5ecef75e6fda23d83deffeffdd544da2103a75422e768d26cfe9ee7f
MD5	2024-05-11	e3eaf28d0259c1b26429966c9b09a3cc
SHA1	2024-05-11	ffa0d8f480c4f39037be40d1eba0a6b6f9016420
MD5	2024-05-11	4d404ac646564376d34cfbabbfe508ec
SHA256	2024-05-11	5ec2650940db1e24271b84e5553d8454f17a7c99cbb36579aa843aa09798efe3
SHA1	2024-05-04	83fdc084031f6ffb1fb3488166100628e1656c65
MD5	2024-05-04	71e04dd1a7ad7068fa236cb7aeb647b3
SHA256	2024-05-04	2889c2834599b95a91d0b4136ed7df199d62e47061dd01d18922d7a7fb15954e
SHA1	2024-05-01	69dd9ef68544298fetc72ea1d9fbd363049d23b3
MD5	2024-05-01	67071b5da1fb59324066982123ed7f68
SHA256	2024-05-01	d938672b5d4f3a25c48474597752ff5f8af36472802a2c6767b2e7dd18506c71
SHA1	2024-04-03	17ef145486c494ea9c727972c501471e720887f0
MD5	2024-04-03	ad997dc4ee32ab469e45009f218175d0

Type	Date Added	Value
SHA256	2024-04-03	a1f8bb5990775f277540eb4c7579695477445afd90262cb819567cc9b3042166
URL	2024-04-02	http://91.92.253.69/3.exe
SHA256	2024-03-23	44f8f0b67907cb91d414a1c0cb33e74e42d201e05869129a9d1d4039dbfb0fe2
MD5	2023-03-21	c7d749686aa87a0826f47179002820dd
MD5	2023-03-21	6b3e8c6d5aa1896241ed1edf73204371
MD5	2023-03-21	24127319213b7e66169c4ea12f44a867
MD5	2023-03-21	d36f15bef276fd447e91af6ee9e38b28
MD5	2023-03-20	da931a33c6dd88f17bd73fad95cc726a
MD5	2023-03-20	93713221ec3d756d1091b3a05d489ef8
MD5	2023-03-20	dffce796a69f576b2ce5161c5bf23249
MD5	2023-03-20	3cfa08af2e428627fc94d12cf816fa84
MD5	2023-03-20	4e37d7cdacd6f2f1fd4bba48a6705705
MD5	2023-03-21	54e737644c21402034c863a89de9f785
SHA256	2023-04-20	6d28fe68df58ab9121992fcdcfba660bac50108c9ea9fd786a8dc3611b4f60289
SHA256	2023-06-29	4364a60cc5f7039a24528452680648850d7b3f434c25892d1b3b5e5aa14898fb
SHA256	2023-07-13	024cce95a63124cd3cbfe3f21fbacf8437fd288717fce379006064aa2a97641e

Type	Date Added	Value
SHA256	2023-07-19	d1e23942effbdf831fb99ceb19495a5338fbcf2872a6782c58b184b4b2b33c4d