Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

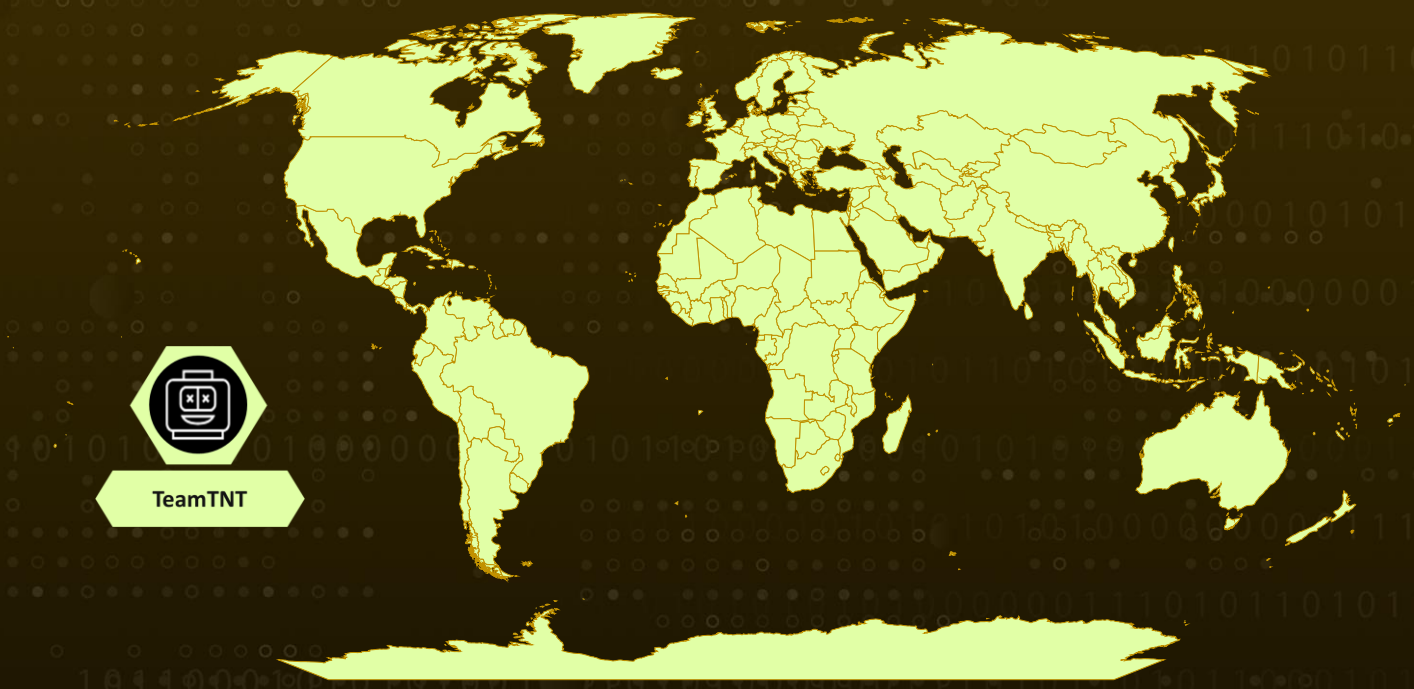
# TeamTNT Reboots with New Weaponry: Rootkits and More

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| September 23, 2024 | A1 | TA2024366 |

# Summary

**First Seen:** October 2019
**Threat Actor:** TeamTNT (aka Adept Libra)
**Malware:** Diamorphine Rootkit
**Affected Platform:** CentOS
**Targeted Region:** Worldwide
**Attack:** TeamTNT is a notorious cybercriminal group, active since 2019, known for targeting cloud and container environments worldwide to deploy cryptocurrency miners. Although they appeared to disband in November 2021 after announcing their exit on Twitter, TeamTNT re-emerged with new cyber campaigns, evolving their capabilities and focusing on Virtual Private Server (VPS) infrastructures running CentOS.

## Attack Regions



# Attack Details

**#1** TeamTNT, a notorious cybercriminal group, gained prominence by targeting cloud and container environments globally. The group is known for exploiting cloud and container resources to deploy cryptocurrency miners within compromised infrastructures.

**#2** Although active since October 2019, TeamTNT appeared to disband after posting a farewell message on Twitter on November 6, 2021, indicating they had ceased operations. However, following a period of inactivity, TeamTNT resurfaced in September 2022 with a series of new cyber campaigns.

**#3** Over time, this threat actor has evolved, enhancing its toolset and expanding its target base while maintaining a low profile. In its latest wave of attacks, TeamTNT has focused on Virtual Private Server (VPS) infrastructures running the CentOS operating system.

**#4** The initial access is achieved through Secure Shell (SSH) brute-force attacks, allowing the group to gain access to victim systems. Post initial access they deployed a malicious script that disables critical security mechanisms, such as SELinux, AppArmor, and firewalls, erases logs, and alters system files while searching for and terminating existing cryptocurrency miners. The group also removes Docker containers and installs the Diamorphine rootkit.

**#5** Diamorphine, a loadable kernel module (LKM) rootkit designed for Linux kernels, enables stealthy control over the compromised system once installed with root privileges. TeamTNT secures its control over the affected system by locking it down, preventing administrators from rebooting, shutting down, or recovering control of the compromised environment.

# Recommendations

**Firewall Configuration:** Allow only essential services through the firewall to minimize the attack surface. Block any unnecessary inbound or outbound connections that could be used by attackers to infiltrate or exfiltrate data.

**Install Fail2Ban:** Use Fail2Ban to automatically detect and block IP addresses exhibiting malicious behavior, such as repeated failed SSH login attempts, reducing the effectiveness of brute-force attacks.

**File Integrity Monitoring and Audit Logging:** Utilize AIDE (Advanced Intrusion Detection Environment) to monitor system files for unauthorized changes, helping you detect signs of intrusion or tampering early. In conjunction, set up Auditd with DISA-STIG recommended rules to actively log changes to system files and configurations.

**Rootkit Detection with rkhunter:** Install and enable rkhunter to regularly scan your system for rootkits, backdoors, and other malicious software that could be used by attackers like TeamTNT to maintain control over your servers.

**Utilize Application Control:** Implement application whitelisting to ensure that only approved applications can run on your systems, preventing unauthorized or malicious executables, such as backdoors, from executing. Additionally, deploy application control solutions that analyze application behavior to detect and block unusual or unauthorized activities.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0001<br>Initial Access | TA0002<br>Execution | TA0003<br>Persistence | TA0004<br>Privilege Escalation |
| TA0005<br>Defense Evasion | TA0006<br>Credential Access | TA0007<br>Discovery | TA0010<br>Exfiltration |
| TA0011<br>Command and Control | TA0040<br>Impact | T1110<br>Brute Force | T1057<br>Process Discovery |
| T1082<br>System Information Discovery | T1105<br>Ingress Tool Transfer | T1083<br>File and Directory Discovery | T1490<br>Inhibit System Recovery |

| | | | |
|---|---|---|---|
| **T1543** Create or Modify System Process | **T1574** Hijack Execution Flow | **T1222** File and Directory Permissions Modification | **T1562** Impair Defenses |
| **T1562.001** Disable or Modify Tools | **T1562.003** Impair Command History Logging | **T1562.004** Disable or Modify System Firewall | **T1562.012** Disable or Modify Linux Audit System |
| **T1070** Indicator Removal | **T1070.006** Timestomp | **T1014** Rootkit | **T1609** Container Administration Command |
| **T1053** Scheduled Task/Job | **T1053.003** Cron | **T1583.003** Virtual Private Server | **T1041** Exfiltration Over C2 Channel |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| IPv4 | 65[.]108[.]48[.]150 |
| File Path | /etc/.system/rtm/xmrig.log, /var/tmp/.../dia, /var/tmp/.../dia/diamorphine.ko, /usr/bin/tntrecht, /var/tmp/.alsp |
| SHA256 | 3be13d69a4c9b94179a6cf45a310acfaa7c5455cba908982fb36277486b5ea86, 3cd21bf96050d89d3bcf8f4d7612c8d60dcc2a9fc2b8764fc6f9c08aabf81c5a, 4a411cf9f0e30eb8c8fd23d38413d2455b0f6e81b0082e749b8ca64cb9ab1e4c, bf46bd921cb615fb7490b50b0ead98ff4ebdbd599eeb3736f568c64f19eab980, d99d7b090da1f1c14a0a554492ba99a506472eab66b057435261a246c2405be5, d947b70347ce1f0088b107a3344c033cdd666782e7b382cd4bccb64724a28575, 4fdadd8b65ce5975745596f9afcd3532d89a80f01e29993ed3842318b56c58b0, 49117f048c668c3d4959796aa447d89899b0ede84dbfb486adb34c92d8cedd2f, 351d0bdab940e0195dd3c5e5da61ea4d46a0cce34a8ea9f78e27b1d233a2486f, |

| TYPE | VALUE |
| --- | --- |
| SHA256 | 69e144206b607522da3b571823f93125d121065ba55c0ead651696a48e92bdcf,<br>ddfdb25d6a30a6d63c705e25e818553fb21ee89f3b988aae7b65c10eec805a1b,<br>b0c4456420e0d650912a99acc9fe4d4eeee9f75921facafc718c2c82ea0365b5,<br>9ba2a5fcc9ab9b229c7d7a139dd1768858738ed3f4ff0e07e23bc59a904188ea1,<br>f79eb2930012ac45e4c4434f8559e0bc40fa269b51fcc297ca4b78c2b61bfcb7,<br>0d0de2151d7fcd14b1bdb64dab802e2290a5a130ba7ed7db6a6e4d5b5b095463,<br>4114d57edae1d877d62d8b5642bd93cfb457b12cf657d53a185e37d09ae51891,<br>91d9421125adceb27e5e40f27a8da6cb5de8971b2e8d081a18020a6c0b44e453,<br>1936270dc97c4e2e7bbdfd0c337ed1acdf72df6dc9598b396f6fdf4c0ad8f904,<br>a158fc3982b8ccbec4655b9a3017eba167e0f0bb61f78f870898a51f7f6076bb,<br>29913a342bca81ec1084c9abc1c6be8d431d0da40fadba465a3ca3481193904b,<br>a931bc92999eeefdcb79bf6dc294608cb825b2d8f2627b1b3ab0b71e74d8d835,<br>5bc5883c31f7e1432663d2f277d6cb2c849cfc1e095bca27bd5d17ff11229fed,<br>8b7eaea5fc2f184ad9ef6abf069bdb78d42662c891b09c3c6a9d4899526b17c8,<br>825b5ab1e44f6744e2fb686c07c145d3b9cbe30e25ba8f6a4b5bf8603c7ecf3a,<br>678d3846429bff6c54e386f65331791e932dd5f2bafc5d0c4877a493cd0ee355,<br>c8e29d0d02610b5d9aa92a13013ea292fd3472cf62ba09f5c1b72ab73619ddc4,<br>afe0498385984eca996d17b37851fdf9213910426f4841da29c6d9c33e98e013,<br>08ffdaafb82fefde776f7e0f9d5824f15cea7ff8043fb7a200e8f4e60a05e82a,<br>e029e90d6767f2b84e9e2d618db105573404d4f09eece52734b9faae5fc25c2c,<br>be40eee5b8b3b3dfa0c453b191ed0fccac9532a41f062c6fcef56db11d366250,<br>5d3373476bcded34f0e2436587254fcc8edab9a771b9a040cbf59c57ab30b4da,<br>b061611f11c620be049ee85651e2950f51e299e91f7488045c5e3b985c769898, |

| TYPE | VALUE |
| --- | --- |
| SHA256 | 44233d8b9de16b9fa0fc1f048300927671a60f03394ad41b0fb7e91a803e4a5c, 5d637915abc98b21f94b0648c552899af67321ab06fb34e33339ae38401734cf, 370fff5098eda6b9ec9ae942c1ce32098e07d7e91d4a5c6e978d8bb22747e6df, 12d6326bd7e7bc8e81e0e161b5537096847253076334bca8c16a3c3f4c2c0e5b, 76c01ef5aaef29e2894beddd8f23726b75f6a8d335499333b60a0e3815de5b2e, 1a9382e491598fea6f418427f36a0e127135ed4886adc846b3339e0505284971, be8e8ef049dedc7c56e7d61f4f50a0ed324a42e1b1febe66aea77156bc6f02a0, 400f3a425ed047442d87ab96e7469f63c6dbc78424771eb2e4b9c305ea44d0b6, d00771a4fd8f314417441d76812466c0a84ab053a8e5960037526d0ff4cba37d, b627725d7f4ee5b969c200c65d61123027df30a8f2b5930c7df5bfbe8a613f6b, 6d388ee0ee34d5ec409c55cee65b8d65aacbfb7f3bf207db47e3fef0d7860877, 954a5905607d1bd1160b6471a36679af9aa57a5fbf777751f68492ecc54d45e1, c2b0588ff7a6d5790cbd5587fc307e6b36a618ccc90c47264b4e1bcc0a549931, 6436303b20b2836d08595a90cfd82806c6dce16f33964aa4749a86b343d0abbb, 8bf0ddff6d2921257fbd3a3791c72fc1ebc7347a84ab4bf0298085d91e5ef0d5, 12360ddc28cfa104377d7c7a92a190933c424c3dd407b65f7b69b1b5c67dca1b, 1fdda23de5a1dbfb70698f2b548c80c1d2967cb0f8d9bba41d64131aaa7532a3 |

## References


https://www.group-ib.com/blog/teamtnt/

https://hivepro.com/threat-advisory/misconfigured-servers-targeted-with-new-golang-malwares/

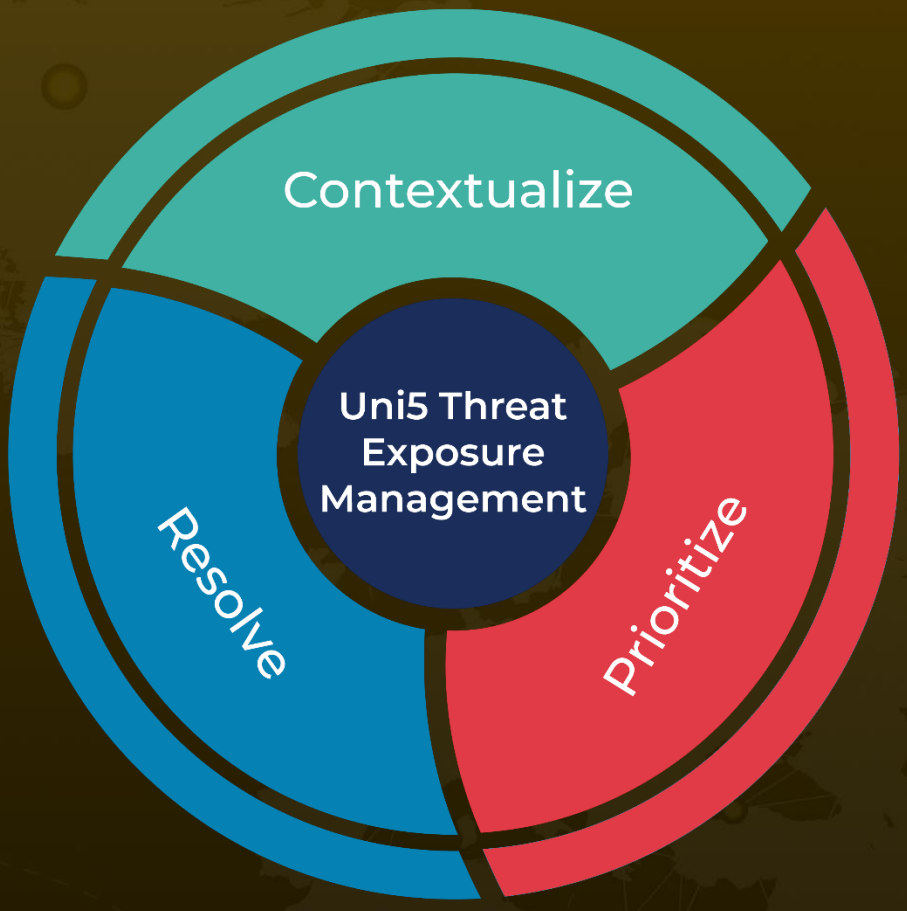
https://hivepro.com/threat-advisory/new-python-based-fileless-malware-named-pyloose-targeting-cloud-environments/

https://attack.mitre.org/groups/G0139/

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**September 23, 2024 • 9:00 PM**



More at www.hivepro.com