Emerging Ransomware BQTLock & GREENBLOOD Disrupt Businesses in Minutes

By ANY.RUN

Published: 2026-02-11 · Archived: 2026-04-05 23:03:48 UTC

How long would it take your team to realize ransomware is already running?

The newly identified ransomware families are already causing real business disruption. These threats can disrupt operations fast while also reducing visibility through stealth or cleanup activity, shrinking the time teams have to detect and contain the attack.

Here's what you should know about BQTLock and GREENBLOOD, and how your team can detect and contain them before the impact escalates.

TL;DR

- **BQTLock** is a stealthy ransomware-linked chain. It injects Remcos into explorer.exe, performs UAC bypass via fodhelper.exe, and sets autorun persistence to keep elevated access after reboot, then shifts into credential theft / screen capture, turning the incident into both ransomware + data breach risk.
- **GREENBLOOD** is a **Go-based** ransomware built for rapid impact: ChaCha8-based encryption can disrupt operations in minutes, followed by self-deletion / cleanup attempts to reduce forensic visibility, plus TOR leak-site pressure to add extortion leverage beyond recovery.
- In both cases, the critical window is **pre-encryption / early execution**: stealth setup (BQTLock) and fast encryption (GREENBLOOD) compress response time and raise cost fast.
- Behavior-first triage in ANY.RUN's Interactive Sandbox lets teams confirm key actions (process injection, UAC bypass, persistence, encryption, self-delete) during execution, extract IOCs immediately, and pivot into Threat Intelligence Lookup (e.g., commandLine:"greenblood") to find related runs/variants and harden detections faster.

BQTLock: A Stealth Attack That Escalates into Data Theft and Business Risk

Original post on LinkedIn

BQTLock is a ransomware-linked threat designed to hide in normal system activity, gain elevated privileges, and quietly prepare for deeper impact before defenders can react.

Instead of triggering obvious alerts immediately, it blends into trusted Windows processes and delays visible damage. This makes early detection difficult and increases the chance of **data exposure, operational disruption, and financial loss** for affected organizations.

How the Attack Was Revealed Through Behavioral Analysis

Using the ANY.RUN interactive sandbox, analysts were able to observe the full behavioral chain in real time.

See full execution chain of BQTLock


BQTLock ransomware analysis
BQTLock attack fully exposed inside ANY.RUN sandbox

The analysis revealed that the malware:

- Injects the Remcos payload into **explorer.exe** to remain hidden inside legitimate system activity
- Performs a **UAC bypass via fodhelper.exe** to obtain elevated privileges
- Establishes autorun persistence to survive system restarts with higher access rights

Once privilege escalation is complete, the threat moves beyond stealth and into active harm, including:

- **data theft capabilities** that increase breach severity
- **screen capture activity** that may expose sensitive corporate information


Credentials stealing by BQTLock
Credentials stealing by BQTLock discovered by ANY.RUN

This sequence shows how quickly a seemingly quiet infection can evolve into a full security and compliance incident.

GREENBLOOD: Fast Encryption, Evidence Removal, and Immediate Business Exposure

Original post on LinkedIn

GREENBLOOD is a newly observed Go-based ransomware built for speed, stealth, and pressure.

Rather than relying only on encryption, it combines rapid file locking, self-deletion to reduce forensic visibility, and data-leak threats through a TOR-based site.
This transforms a technical incident into a full business crisis involving downtime, regulatory exposure, reputational damage, and recovery cost.

For organizations, the biggest risk is timing. By the moment encryption becomes visible, sensitive data may already be stolen and operational disruption already underway.

How the Attack Was Uncovered During Real-Time Detection and Triage

Inside the ANY.RUN interactive sandbox, ransomware behavior and cleanup activity became visible while execution was still unfolding, allowing early detection during the most critical stage of the attack.

Check full attack chain of GREENBLOOD

GREENBLOOD exposed inside ANY.RUN sandbox in around 1 minute

The sandbox analysis exposed:

- **Fast ChaCha8-based encryption** capable of disrupting operations within minutes
- **Attempts to delete the executable**, limiting post-incident forensic visibility
- **Actionable indicators of compromise** that enable earlier detection across endpoints and environments

Because this behavior is captured in real time, SOC teams can move directly from **detection to triage and containment** before encryption spreads widely.

Using ANY.RUN Threat Intelligence, teams can search for other sandbox analyses related to GREENBLOOD and track how the threat appears across different environments. A simple query like helps uncover related executions, recurring patterns, and potential variants that may not match the exact same sample.

Use this query link to explore related activity: **commandLine:"greenblood"**

Sandbox analyses related to GREENBLOOD displayed by TI Lookup for deeper investigation

This is valuable as ANY.RUN Threat Intelligence is connected to real sandbox activity from **15,000+ organizations** and **600,000+ security professionals**. In practice, that means you can use community-scale execution evidence to strengthen detections faster, tune response playbooks, and stay ahead as ransomware changes.

How These Ransomware Attacks Impact Businesses

BQTLock and GREENBLOOD may use different techniques, but they point to the same operational reality: modern ransomware is designed to create maximum business damage in the shortest possible time.

Instead of slow, visible attacks, today's ransomware combines stealth, speed, privilege escalation, and data-leak pressure to overwhelm traditional response workflows before containment begins.

Business risk	**BQTLock**	**GREENBLOOD**
Data exposure risk	Data theft + screen capture after escalation	Leak-site pressure adds exposure risk (even post-recovery)
Downtime risk	Can escalate after stealth phase	Fast encryption (ChaCha8)
Harder to spot early	Hides in normal processes + persistence	Cleanup/self-deletion attempts
Extortion pressure	Can intensify if stolen data is used	TOR leak-site threats
Short response window, higher cost	Stealth setup compresses reaction time	Fast encryption compresses reaction time

For most companies, the fallout comes in a few predictable ways:

- **Data theft before encryption:** After privilege escalation, BQTLock moves into data theft and screen capture, turning ransomware into a breach and compliance issue.
- **Disruption in minutes:** GREENBLOOD encrypts fast, which can cause rapid downtime and immediate operational impact.
- **Stealth and cleanup slow response:** BQTLock hides in normal processes and persists with elevated rights, while GREENBLOOD attempts self-deletion, reducing visibility and increasing recovery cost.
- **Extortion pressure beyond recovery:** GREENBLOOD includes **leak-site threats** via a TOR-based platform. That adds a second layer of pressure: even if systems are restored, the business may still face data exposure, compliance issues, and long-term brand damage.
- **Short response window, higher cost:** Between stealth setup and fast encryption, delays quickly translate into bigger financial damage.

How SOC Teams Can Detect and Contain Modern Ransomware Before It Spreads

Stealthy privilege escalation, rapid encryption, and leak-site extortion leave security teams with very little time to react.

To stop ransomware before it reaches full business impact, SOC teams need an operational cycle that moves from early detection → confirmed behavior → broader visibility → proactive defense in minutes,
without any complicated steps and setups.

With ANY.RUN, this cycle happens inside a single connected workflow, allowing teams to shift from late response to early containment.

1. Confirm Ransomware Behavior Before Encryption Spreads

The first and most critical step is safe behavioral detonation.

Ransomware like BQTLock hides inside trusted processes and escalates privileges quietly. GREENBLOOD encrypts files quickly and attempts to remove traces.

Running suspicious files or links inside ANY.RUN's controlled environment exposes:

- privilege escalation attempts
- persistence mechanisms
- encryption activity
- data theft or screen capture behavior


Encryption activity performed by GREENBLOOD

Encryption activity performed by GREENBLOOD revealed inside ANY.RUN sandbox

As this visibility appears during execution, teams can reach a clear verdict in seconds instead of discovering the attack after downtime begins.

This early proof translates directly into operational gains, with 94% of teams reporting **faster triage**, Tier-1 to Tier-2 **escalations reduced** by up to 30%, and **MTTR shortened** by an average of 21 minutes per case, helping contain ransomware before downtime and financial impact grow.

2. Expand Investigation Using Real-World Threat Intelligence

Stopping a single sample is not enough if the campaign continues elsewhere.

Indicators extracted from sandbox analysis can be used to search across ANY.RUN Threat Intelligence, revealing:

- related ransomware executions
- reused infrastructure or tooling
- emerging variants and evolving tactics

The payoff is earlier campaign-level detection and clearer evidence for decision-making, which **lowers breach exposure**, strengthens compliance readiness, and **reduces the business impact** of repeat attacks.

3. Strengthen Prevention and Reduce Future Incident Cost

The final step is turning investigation insight into ongoing protection.

Fresh indicators and behavioral signals can flow directly into your existing stack through ANY.RUN TI Feeds, keeping detections current without manual copy-paste or constant rule rewrites. This helps teams block repeat attempts faster and react to shifting ransomware infrastructure as it changes.


TI Feeds delivering fresh IOCs

TI Feeds delivering fresh IOCs to your existing stack for proactive monitoring

This ongoing flow shifts teams from reactive detection to **proactive monitoring**, so attacks are discovered earlier and contained with less business impact.

About ANY.RUN

ANY.RUN is part of modern SOC workflows, integrating easily into existing processes and strengthening the entire operational cycle across Tier 1, Tier 2, and Tier 3.

It supports every stage of investigation, from exposing real behavior during safe detonation, to enriching analysis with broader threat context, and delivering continuous intelligence that helps teams move faster and make confident decisions.

Today, more than 600,000 security professionals and 15,000 organizations rely on ANY.RUN to accelerate triage, reduce unnecessary escalations, and stay ahead of evolving phishing and malware campaigns.

To stay informed about newly discovered threats and real-world attack analysis, follow ANY.RUN's team on **LinkedIn** and **X**, where weekly updates highlight the latest research, detections, and investigation insights.

Frequently Asked Questions

What makes BQTLock and GREENBLOOD different from traditional ransomware?

Both strains prioritize early stealth and rapid operational impact rather than delayed, obvious encryption. BQTLock focuses on covert privilege escalation, persistence, and data theft before encryption, while GREENBLOOD delivers fast ChaCha8 encryption, self-deletion, and leak-site extortion, compressing the response window to minutes.

Why is the pre-encryption stage critical for detection?

Modern ransomware often causes business damage before files are encrypted. Activities like process injection, UAC bypass, credential theft, and data exfiltration signal compromise early. Detecting these behaviors during execution enables containment before downtime, breach disclosure, or financial loss escalate.

How does GREENBLOOD achieve such fast disruption?

GREENBLOOD is Go-based and uses ChaCha8 encryption, allowing it to lock files quickly across the system. It also attempts self-deletion and cleanup, which reduces forensic visibility and increases recovery complexity while applying TOR-based leak pressure on victims.

What indicators should SOC teams monitor for BQTLock activity?

Key signals include Remcos injection into explorer.exe, UAC bypass via fodhelper.exe, autorun persistence creation, and post-escalation credential theft or screen capture. These behaviors indicatethe attack is transitioning from stealth access to active breach risk.

How can security teams confirm ransomware behavior faster?

Running suspicious files or links in a controlled behavioral sandbox allows teams to observe privilege escalation, persistence, encryption, and cleanup actions in real time, extract IOCs immediately, and begin containment and hunting before the attack spreads.

How does threat intelligence help reduce repeat incidents?

Linking sandbox-derived indicators to broader execution telemetry reveals related samples, reused infrastructure, and evolving variants. Feeding this intelligence into detection controls supports earlier blocking, stronger prevention, and lower long-term incident cost.
