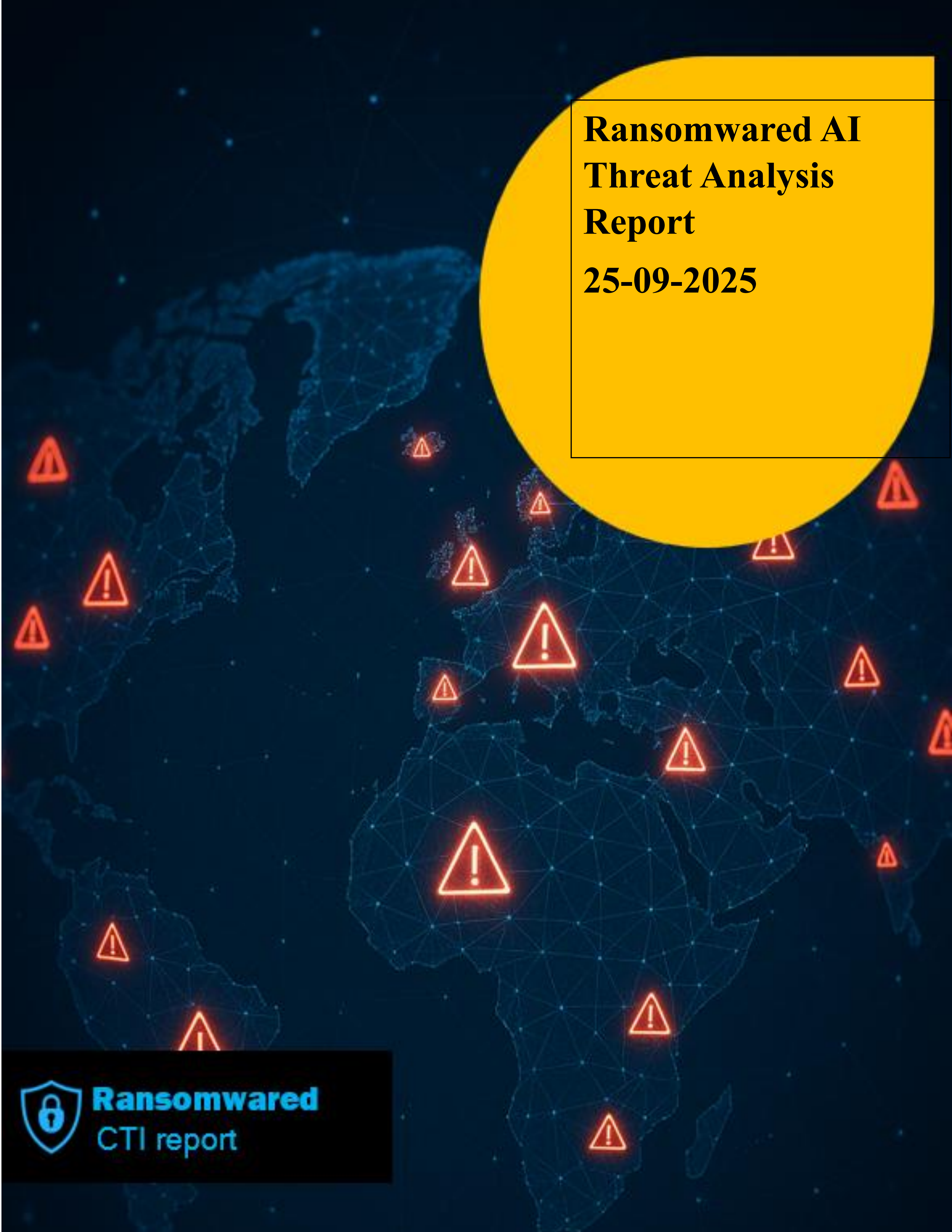
Ransomwared AI Threat Analysis Report

25-09-2025



Ransomwared
CTI report

1. Management Summary

Ransomwared AI has detected and analyzed malicious activity stemming from a trojanized installer delivered through a **ClickUp file-sharing link**. The file, named `flameshot.msi`, was presented as an installer for a legitimate open-source utility but was in fact a **multi-stage malware loader**. Once executed, the installer unpacked and deployed several payloads including `setup.exe`, `nsy4F00.tmp.exe`, `pcappstore.exe`, and `watchdog.exe`, as well as malicious dynamic link libraries (`NSISFastLib.dll`).

At its core, this incident demonstrates the **evolving sophistication of malware distribution campaigns**. Attackers are increasingly abusing trusted platforms, such as SaaS collaboration tools, to deliver payloads in ways that bypass traditional perimeter defenses. By naming the file after legitimate software, adversaries exploited trust and familiarity, dramatically increasing the likelihood of execution.

From a tactical perspective, the malware exhibited a **layered infection chain**:

- **Initial Access** through a malicious MSI hosted on ClickUp.
- **Execution** of NSIS-based temporary payloads.
- **Persistence** via `watchdog.exe`, ensuring that the infection survives reboots.
- **Defense Evasion** through deletion of temporary files, DLL cleanup, and the abuse of **Living-off-the-Land Binaries (LOLBINs)** such as `UI0Detect.exe` and `Google\updater.exe`.
- **Command-and-Control (C2)** communications masquerading as legitimate connections to Microsoft, Google, and Let's Encrypt infrastructure.

The use of LOLBINs is particularly concerning. By injecting into or executing through trusted signed binaries, the malware blends malicious behavior with normal system operations, making detection far more difficult. Many traditional antivirus solutions whitelist these binaries, which gives attackers a stealthy persistence mechanism.

The **business implications** of this incident are significant. While some observed components (`pcappstore.exe`) resemble adware or nuisance-level software, the infection framework is modular and capable of delivering **additional payloads at any time**. This means what begins as a seemingly minor intrusion could escalate into credential theft, lateral movement, or even a ransomware attack. For organizations subject to regulatory frameworks like GDPR, NIS2, or ISO 27001, such an incident could trigger breach notification requirements if data exposure occurs.

The **network behavior** of this malware further reinforces its stealthy design. By directing outbound traffic to domains associated with CDNs and PKI validation (`res.public.onecdn.static.microsoft`, `c.pki.goog`), the adversaries ensured that their traffic would appear legitimate to most monitoring tools. Blocking such traffic outright is impractical in enterprise settings, meaning defenders must rely on behavioral analysis, anomaly detection, and endpoint telemetry to identify malicious usage.

Ransomwared AI's assessment is clear: this incident is not a one-off infection but a manifestation of a **modular loader framework designed for persistence and escalation**. The presence of a watchdog process, the abuse of LOLBINs, and disguised C2 traffic all point to a deliberate attempt to secure long-term access within an environment. Left unchecked, this type of malware provides attackers with an adaptable foothold from which they can pivot to more destructive actions, including ransomware deployment.

In conclusion, this case should serve as a warning that modern malware is **no longer noisy or obvious**. Attackers rely on trusted platforms, trusted binaries, and stealthy techniques to evade detection and maintain control. Organizations must treat such detections with the utmost seriousness, applying not just containment and eradication but also strategic improvements to monitoring and defense.

Ransomwared AI verdict: High-risk, persistent malware leveraging LOLBINs, SaaS distribution, and modular payload delivery. Immediate remediation and long-term defensive adjustments are recommended.

2. Observed Components

During the course of analysis, Ransomwared AI identified several distinct components that together form the infection chain. Each serves a unique role, from initial access to persistence, and demonstrates the modular design of the campaign.

1. **`setup.exe` (SHA256: 38ed2cad40f88de369a22ed6bbbfb6f7670c639eee3b3d9881b572ec7ca99713)**
   This is the initial executable responsible for unpacking and triggering the malware chain. Built with the Nullsoft Scriptable Install System (NSIS), it appears outwardly as a benign installer. However, it drops additional payloads into the `%TEMP%` directory and initiates their execution. This file marks the **entry point** into the infection.
2. **`nsy4F00.tmp.exe` (SHA256: fefe03f1eeb84fa789e475d5d34482071bcbd37a)**
   Generated during the installation process, this file represents the **temporary stage-two loader**. Its naming convention is typical of NSIS unpacked executables, which attackers exploit to disguise malicious files as normal system artifacts. Once active, it begins loading malicious DLLs (`NSISFastLib.dll`) and coordinating further payload execution.
3. **`pcappstore.exe` (SHA256: 246cc59d39961e9c21b73b5d98083e2f76b01c2a)**
   This binary masquerades as a legitimate utility. Its functionality aligns with **adware and downloader behavior**, likely intended for monetization or as a placeholder for more malicious downloads. By presenting itself as a “PC App Store,” it leverages user trust to avoid suspicion. Its true purpose is to expand the infection footprint and enable future payload delivery.
4. **`watchdog.exe` (SHA256: 7f74c62b59a0cf2aa03802e7ff083dc4697b24e1)**
   The watchdog process is explicitly designed for **persistence**. It continuously monitors other malicious executables and ensures they are relaunched if terminated. This functionality guarantees long-term infection and complicates remediation efforts. Even if defenders manually terminate the malware, the watchdog reinstates it.
5. **`NSISFastLib.dll` (multiple variants in `%TEMP%`)**
   These DLLs are dropped and executed in memory during runtime. They support malicious activity such as **process injection, registry modification, and system discovery**. After use, they are deleted from disk, demonstrating both anti-forensic intent and defense evasion.

The interplay between these components highlights a **layered and resilient strategy**. The loader (`setup.exe`) provides the initial infection, the temporary stage (`nsy4F00.tmp.exe`) bridges execution, `pcappstore.exe` introduces monetization or expansion, and `watchdog.exe` ensures survival. DLL components facilitate stealth and evasion. This modularity means the adversary can easily swap or add payloads, making the framework adaptable to different objectives.

Delivery Vector

Ransomwared AI traced the origin of `nsy4F00.tmp.exe` to an external download hosted on a **ClickUp file-sharing link**:

```
https://t90151177714.p.clickup-attachments.com/t90151177714/2e960bff-8584-4528-8cc1-
fd3ec8cd7042/flameshot.msi
```

The file name (`flameshot.msi`) masquerades as an installer for the legitimate Flameshot screenshot tool. Instead, this MSI package acts as a **trojanized installer**. Upon execution, it unpacks `nsy4F00.tmp.exe` into a temporary directory and launches it.

This method demonstrates **two key adversary strategies**:

- **Abuse of trusted SaaS providers** – Traffic to ClickUp is typically whitelisted or implicitly trusted. Delivering malware through such channels bypasses email security and perimeter filtering.
- **Masquerading as legitimate software (ATT&CK T1036)** – Using the name of a real open-source project increases the chance of execution by unsuspecting users.

The delivery mechanism therefore represents not only an infection source but also a significant **security gap**: attackers are exploiting everyday business tools as malware distribution platforms.

Observed Components

During analysis, **Ransomwared AI** identified multiple files associated with the infection chain. Each of these plays a distinct role in establishing the compromise, ensuring persistence, or disguising malicious activity. Understanding their function is essential to grasping how the malware operates as a modular framework rather than a single executable threat.

File Name	SHA256 Hash	Ransomwared AI Assessment
`setup.exe`	38ed2cad40f88de369a22ed6bbbfb6f7670c639eee3b3d9881b572ec7ca99713	Initial installer / loader
`nsy4F00.tmp.exe`	fefe03f1eeb84fa789e475d5d34482071bcbd37a	NSIS unpacked stage payload
`pcappstore.exe`	246cc59d39961e9c21b73b5d98083e2f76b01c2a	Adware / downloader module
`watchdog.exe`	7f74c62b59a0cf2aa03802e7ff083dc4697b24e1	Persistence watchdog
`NSISFastLib.dll`	(multiple temp paths)	Malicious DLL executed in memory

1. **`setup.exe` (SHA256: 38ed2cad40f88de369a22ed6bbbfb6f7670c639eee3b3d9881b572ec7ca99713)**
    - This file acts as the initial loader. To an unsuspecting user, it presents itself as a standard software installer, but in reality, it is built with **NSIS (Nullsoft Scriptable Install System)**. Attackers often use NSIS to wrap malicious payloads because it is widely recognized as a legitimate packaging tool. Once executed, `setup.exe` unpacks additional components into temporary directories and triggers the execution of subsequent stages.
2. **`nsy4F00.tmp.exe` (SHA256: fefe03f1eeb84fa789e475d5d34482071bcbd37a)**
    - This file is a **temporary stage payload** created during the NSIS installation routine. Its naming convention (`nsy*.tmp.exe`) is typical of automatically generated files during NSIS installer execution. Attackers leverage this behavior to hide in plain sight—administrators who see such files may dismiss them as harmless leftovers. However, this binary plays a critical role in

continuing the infection by loading DLLs, injecting into processes, and preparing persistence mechanisms.

3. **`pcappstore.exe` (SHA256: 246cc59d39961e9c21b73b5d98083e2f76b01c2a)**
    - Once the environment has been staged, this executable is deployed as a **secondary payload**. It pretends to be a utility related to a "PC App Store," but its actual behavior aligns with **adware and downloader functionality**. It is likely designed to monetize the infection by delivering unwanted applications or by serving as a flexible module for retrieving more serious malware at a later stage. Even if the initial activity appears limited to nuisance software, the capability to download new payloads makes it highly dangerous.
4. **`watchdog.exe` (SHA256: 7f74c62b59a0cf2aa03802e7ff083dc4697b24e1)**
    - This binary is dedicated to **persistence**. As the name suggests, `watchdog.exe` monitors the other components and ensures they are relaunched if terminated. Such a process drastically increases the difficulty of remediation, since simply deleting the loader or secondary payloads may not be sufficient—`watchdog.exe` will attempt to restore them. This reflects a deliberate design choice by the attackers to guarantee long-term presence.
5. **`NSISFastLib.dll` (various temp paths)**
    - Several DLLs under this name were unpacked into temporary directories during execution. They are loaded into memory and immediately leveraged for malicious tasks such as process injection, system discovery, and registry manipulation. After execution, many of these DLLs were deleted, a behavior consistent with **anti-forensics and defense evasion**.

Together, these components demonstrate a **layered strategy**: a trusted-looking installer delivers temporary files, which in turn deploy adware and persistence modules, all reinforced by DLLs that execute stealthily in memory. The infection chain is resilient, deceptive, and capable of expansion.

3. MITRE ATT&CK Mapping

Ransomwared AI mapped the observed behaviors against the **MITRE ATT&CK framework**, which provides a standardized taxonomy for adversary tactics, techniques, and procedures (TTPs). The following tactics were identified during analysis of the infection chain:

Execution (TA0002)

The malware relied on multiple execution vectors. The initial loader (`setup.exe`) unpacked temporary payloads (`nsy4F00.tmp.exe`) which were subsequently executed. Additional binaries such as `pcappstore.exe` and `watchdog.exe` were also launched. Notably, the malware abused **Living-off-the-Land Binaries (LOLBINs)** including `UI0Detect.exe` and `Google\updater.exe`. By hijacking legitimate executables, the attackers were able to run malicious code under the guise of trusted processes, reducing the likelihood of immediate detection.

Persistence (TA0003)

Persistence was achieved through the deployment of `watchdog.exe`, a binary specifically designed to ensure the continued operation of the malware. This process monitored other malicious components and relaunched them if terminated. The watchdog functionality ensures the infection remains active across reboots and complicates remediation efforts.

Privilege Escalation (TA0004)

Privilege escalation was observed through **process injection** into `Google\updater.exe`. Since this executable is both signed and trusted, injecting into it allows malicious code to inherit the privileges and legitimacy of the host process, bypassing some endpoint protections.

Defense Evasion (TA0005)

The campaign employed several evasion techniques. Temporary files and DLLs were deleted after use to limit forensic evidence. DLLs such as `NSISFastLib.dll` were executed in memory and then removed, demonstrating anti-forensics behavior. Sandbox detection was attempted using timing checks (`GetTickCount`), while LOLBIN abuse provided further camouflage, making the malware blend into normal system operations.

Discovery (TA0007)

Registry keys were queried, particularly those under `FipsAlgorithmPolicy` and personalization settings. This indicates discovery activity, as attackers may be testing system configurations to evaluate cryptographic policy enforcement and user environment details before selecting further payloads.

Collection (TA0009)

DLL injection into memory-resident processes provided a means to collect local data. While no explicit data exfiltration was observed in this stage, the capabilities are consistent with information gathering and staging for later theft.

Command & Control (TA0011)

Outbound communications were established to domains and IPs associated with Microsoft, Google, and Akamai infrastructure. While these endpoints are legitimate, the malware used them to disguise **command-and-**

control (C2) traffic as ordinary update and certificate activity. This masquerading strategy makes detection at the network level far more challenging.

Impact (TA0040)

Finally, the malware demonstrated potential impact by tampering with **cryptographic policies** in the registry. This could weaken the host’s security configuration, enabling follow-on attacks. In addition, the modular loader framework observed here is well-suited to stage more destructive payloads such as ransomware, which would directly affect availability and business continuity.

4. Ransomwared AI Network Findings

The network telemetry collected during analysis reveals a two-phase pattern: **initial delivery** from a cloud collaboration service, followed by **command-and-control (C2) communications** disguised as legitimate system traffic. This combination highlights the adversaries' strategy of leveraging both **trusted SaaS platforms** and **trusted infrastructure** to evade detection.

Malicious Delivery Link

The temporary payload `nsy4F00.tmp.exe` was downloaded via a ClickUp attachment masquerading as a legitimate installer:

```
https://t90151177714.p.clickup-attachments.com/t90151177714/2e960bff-8584-4528-8cc1-
fd3ec8cd7042/flameshot.msi
```

This MSI pretended to be an installer for the open-source tool *Flameshot* but in fact acted as a dropper. By distributing the file through **ClickUp's trusted domain**, the attackers bypassed perimeter defenses, since SaaS traffic to collaboration tools is rarely blocked.

Resolved IP Address for Delivery:

- `34.120.22.50` (ClickUp infrastructure – at time of analysis)

This IP may vary over time due to CDN or cloud hosting changes, but the finding underscores how adversaries exploit SaaS providers as a delivery channel.

C2 and Post-Infection Communications

Once the payload executed, the malware initiated connections to domains normally associated with content delivery and PKI validation:

- `res.public.onecdn.static.microsoft`
- `c.pki.goog`
- `crl.root-x1.letsencrypt.org.edgekey.net`
- `e8652.dscx.akamaiedge.net`
- `x1.c.lencr.org`

These domains resolved to multiple IPs during analysis, including:

- `104.71.214.69:80`
- `151.101.22.172:80`
- `20.69.140.28:443`
- `23.196.145.221:80`
- `23.46.228.49:443`
- `23.196.193.245:80`

Traffic was observed over both HTTP and HTTPS. Because these destinations belong to trusted providers, the adversary gains stealth: defenders cannot easily block or blacklist them without disrupting legitimate business operations.

Ransomwared AI Assessment

- **Initial Access**: Abuse of a SaaS provider (ClickUp) for payload delivery.
- **Persistence of C2**: Ongoing communications hidden within traffic to Microsoft, Google, Akamai, and Let’s Encrypt.
- **Risk**: Traditional network defenses will struggle to distinguish between legitimate update traffic and malicious activity without deeper endpoint-to-network correlation.

Business Impact

This blended use of SaaS and CDN traffic creates a **high-risk blind spot**. Attackers can both deliver initial payloads and maintain C2 channels without triggering basic network defenses. Organizations must therefore rely on **behavioral monitoring** and **EDR telemetry** to spot anomalies rather than depending solely on static domain or IP blocklists.

5. File System & Registry Activity

The forensic evidence collected by **Ransomwared AI** shows that the malware campaign relies heavily on **temporary file creation, DLL injection, and registry interaction** to maintain functionality while concealing its tracks. This section summarizes the key file system and registry behaviors observed during execution.

File System Activity

Once launched, the trojanized installer (`flameshot.msi` → `setup.exe`) unpacked multiple artifacts into the user's profile directories, particularly under `%TEMP%` and `%APPDATA%`. These included:

- **Temporary executables**: `nsy4F00.tmp.exe` and related NSIS unpacked files.
- **Dynamic link libraries (DLLs)**: Multiple instances of `NSISFastLib.dll` dropped under random temp subfolders.
- **Persistence artifacts**: `watchdog.exe` was installed to ensure reinfection if components were removed.

Observed behaviors included:

- **File Creation**: Malicious DLLs were repeatedly written to `%TEMP%` and loaded into memory.
- **File Deletion (Anti-Forensics)**: After use, the malware deleted many temporary files and DLLs, attempting to erase forensic evidence. For example, temp folders like `nslBE7E.tmp\` and DLLs such as `NSISFastLib.dll` were explicitly removed.
- **File Overlap**: Legitimate-looking folders (e.g., `Microsoft\Windows\Caches`) were accessed and modified, potentially to hide artifacts among normal system files.

This combination of **write–execute–delete cycles** reflects a strategy to minimize detection while ensuring successful execution.

Registry Activity

The malware accessed and manipulated several registry keys during execution. Most notably:

- **Cryptographic Policy Keys**:
  - `HKLM\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy`
  - Values such as `Enabled`, `MDMEnabled`, and `STE` were accessed.
  - **Impact**: By tampering with FIPS algorithm policies, attackers could weaken or alter system cryptographic enforcement, lowering the overall security baseline.
- **Personalization Settings**:
  - `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\Personalize`
  - Keys like `AppsUseLightTheme` were queried.
  - **Assessment**: These queries may serve as **sandbox evasion checks** (e.g., detecting default environments versus real user profiles).
- **RPC and GDI-related Keys**:
  - `HKLM\SOFTWARE\Microsoft\Rpc\Extensions\NdrOleExtDLL`
  - `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize`
  - These may be used for further persistence or system discovery.

Ransomwared AI Assessment

The file system activity demonstrates a **classic loader pattern**: unpacking payloads into writable locations, executing them, and then deleting evidence. Registry interaction indicates both **defense evasion** (detecting sandbox conditions) and **system weakening** (tampering with crypto policies).

Business Impact

File and registry manipulation creates multiple risks:

- **System Integrity**: Altered cryptographic settings could undermine compliance and weaken data protection.
- **Forensic Challenges**: File deletion reduces the availability of artifacts, making incident response more complex.
- **Persistence**: The placement of watchdog executables in user-accessible directories ensures long-term survival of the malware.

6. Living-off-the-Land Abuse

One of the most concerning aspects of this campaign, as observed by **Ransomwared AI**, is its deliberate abuse of **Living-off-the-Land Binaries (LOLBINs)**. LOLBINs are legitimate executables already present on the system—often digitally signed and trusted—that attackers hijack to execute malicious code. This allows adversaries to blend their activity into normal system operations, effectively **turning the system's own trusted tools against itself**.

Key LOLBINs Abused

1. **`Google\updater.exe`**
    - Normally used to update Google applications such as Chrome.
    - The malware injected malicious code into this signed, trusted binary.
    - **Impact**: By running inside `updater.exe`, the malware inherits the trust associated with a legitimate vendor process. Security products that whitelist signed binaries may overlook the injected malicious behavior.
2. **`UI0Detect.exe`**
    - A native Windows binary responsible for detecting interactive service sessions.
    - The malware launched this process as part of its execution flow.
    - **Impact**: Running within a Windows core component enables the malware to masquerade as legitimate system activity, reducing suspicion.

Tactics Enabled by LOLBIN Abuse

- **Defense Evasion**: By hiding inside trusted binaries, the malware avoids detection from traditional antivirus or application control solutions that focus on unknown or unsigned executables.
- **Privilege Escalation**: Execution within processes like `updater.exe` can grant the malware elevated privileges, enabling it to perform actions not normally available to standard user processes.
- **Persistence**: As long as these binaries remain present, attackers can continue to re-inject or re-execute their payloads, ensuring long-term survival.
- **Blended Traffic**: Malicious communications leaving the host under the guise of legitimate processes further complicates network-based detection.

Ransomwared AI Assessment

The reliance on LOLBINs is a hallmark of **advanced and stealthy campaigns**. Rather than relying solely on custom executables—which are more likely to be flagged and quarantined—the adversaries leveraged what the system already trusts. This strategy demonstrates a high level of operational awareness and increases the difficulty of detection and eradication.

Business Impact

- **Detection Gaps**: Security teams relying on traditional antivirus may fail to see malicious activity since it runs within signed binaries.
- **Incident Complexity**: Forensic investigations become more difficult, as analysts must differentiate between legitimate binary execution and injected code.
- **Increased Resilience**: The malware gains a longer operational window to carry out theft, persistence, or even ransomware deployment.

By abusing LOLBINs such as `Google\updater.exe` and `UI0Detect.exe`, the attackers ensured that their activity would blend seamlessly into everyday system behavior—making this campaign particularly dangerous.

7. Indicators of Compromise (Ransomwared AI Verified)

As part of this investigation, **Ransomwared AI** compiled a set of **Indicators of Compromise (IoCs)** that can be used by defenders to detect, block, or hunt for related malicious activity in their environments. These IoCs cover file hashes, file system paths, registry activity, network infrastructure, and delivery artifacts. While individual indicators may change over time due to malware updates, their combined presence is a strong sign of compromise.

File Hashes (Malicious Binaries)

- `38ed2cad40f88de369a22ed6bbbfb6f7670c639eee3b3d9881b572ec7ca99713` → `setup.exe` (initial loader)
- `fefe03f1eeb84fa789e475d5d34482071bcbd37a` → `nsy4F00.tmp.exe` (NSIS stage payload)
- `246cc59d39961e9c21b73b5d98083e2f76b01c2a` → `pcappstore.exe` (adware/downloader)
- `7f74c62b59a0cf2aa03802e7ff083dc4697b24e1` → `watchdog.exe` (persistence component)

File System Paths

- `%TEMP%\nsy4F00.tmp.exe`
- `%TEMP%\*\NSISFastLib.dll` (multiple variants in temp subfolders)
- `%APPDATA%\watchdog.exe`
- `%PROGRAMFILES%\pcappstore\pcappstore.exe`

Registry Keys Accessed

- `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\Personalize`
- `HKLM\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy`
- `HKLM\SOFTWARE\Microsoft\Rpc\Extensions\NdrOleExtDLL`
- `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize`

These keys were accessed or modified during execution. Particularly concerning is the interaction with **FIPS algorithm policies**, which could weaken cryptographic enforcement.

Delivery Vector (External)

- Malicious download masquerading as a legitimate installer:
  - `https://t90151177714.p.clickup-attachments.com/.../flameshot.msi`
- Resolved delivery IP (ClickUp infrastructure at time of analysis):
  - `34.120.22.50`

C2 Domains and Infrastructure

- `res.public.onecdn.static.microsoft`
- `c.pki.goog`
- `crl.root-x1.letsencrypt.org.edgekey.net`
- `e8652.dscx.akamaiedge.net`
- `x1.c.lencr.org`

Resolved IPs during execution:

- `104.71.214.69:80`

- `151.101.22.172:80`
- `20.69.140.28:443`
- `23.196.145.221:80`
- `23.46.228.49:443`
- `23.196.193.245:80`

Ransomwared AI Guidance

- **Detection**: Import hashes into SIEM/EDR platforms and search for historical presence.
- **Hunting**: Monitor for unusual DLL creation/deletion in `%TEMP%`, registry access to `FipsAlgorithmPolicy`, and outbound traffic to the listed IPs/domains.
- **Blocking**: Hash- and path-based blocking should be combined with behavioral detection, since attackers may rotate infrastructure or recompile binaries.

Together, these IoCs provide defenders with actionable intelligence to identify and contain infections, even in cases where the malware attempts to disguise its activity as legitimate system behavior.

8. Ransomwared AI Conclusion

The analysis conducted by **Ransomwared AI** demonstrates that the identified malware campaign is not a simple nuisance infection but a **sophisticated, multi-stage loader framework** designed to persist, evade detection, and potentially escalate into far more destructive operations.

At the start of the chain, a trojanized installer (`flameshot.msi`) was delivered via **ClickUp's file-sharing platform**, exploiting trust in collaboration tools to bypass perimeter defenses. Once executed, the installer unpacked secondary payloads (`setup.exe`, `nsy4F00.tmp.exe`), which in turn deployed additional binaries including `pcappstore.exe` and `watchdog.exe`. Together with malicious DLLs (`NSISFastLib.dll`), these components created a **layered infection model** in which each stage reinforced the next.

The malware's reliance on **Living-off-the-Land Binaries (LOLBINs)** such as `Google\updater.exe` and `UI0Detect.exe` represents one of the most critical findings. By injecting code into or executing through trusted, signed system binaries, the attackers ensured their activity would blend in with normal operations. This tactic makes it far more difficult for defenders relying on traditional antivirus or application whitelisting to detect the compromise.

Network telemetry further reinforced the campaign's stealthy design. Outbound communications were directed toward infrastructure owned by Microsoft, Google, Akamai, and Let's Encrypt—services that organizations normally trust implicitly. By hiding C2 traffic within such traffic flows, the adversaries gained an operational advantage: defenders cannot simply block these domains without also disrupting legitimate business activity.

From a security posture perspective, the malware poses **critical risks** in three domains:

1. **Persistence** – The watchdog process and LOLBIN injection guarantee long-term survival.
2. **Stealth** – File deletion, DLL cleanup, and trusted infrastructure abuse complicate detection and response.
3. **Escalation Potential** – While some payloads resemble adware, the framework is fully capable of delivering ransomware or data-theft modules.

Business impact should not be underestimated. Beyond immediate remediation costs, organizations risk compliance exposure (GDPR, NIS2, ISO 27001), reputational damage, and operational disruption if such infections are left unchecked.

In summary, this incident highlights the **modern evolution of malware**: no longer relying on noisy executables, but instead abusing trusted platforms, trusted binaries, and legitimate services to silently embed themselves within enterprise environments. Swift containment, thorough eradication, and long-term strategic improvements are required to neutralize this threat.

9. Recommendations

In response to the observed intrusion, **Ransomwared AI** recommends a structured remediation approach that balances **immediate containment**, **systematic eradication**, and **strategic improvements** to prevent recurrence.

Short-Term (Immediate Containment)

1. **Isolate Affected Hosts**
    - Immediately remove compromised systems from the network to prevent further C2 communications or lateral movement.
    - Disable both wired and wireless connectivity until forensic imaging is complete.
2. **Block IoCs**
    - Ingest the provided file hashes, file paths, registry keys, domains, and IP addresses into SIEM/EDR platforms.
    - Establish temporary firewall rules to block outbound connections to identified infrastructure (e.g., Akamai/Let's Encrypt C2 lookalikes).
3. **Suspend Malicious Processes**
    - Terminate `watchdog.exe`, injected `updater.exe` processes, and any temporary executables such as `nsy4F00.tmp.exe`.
    - Verify removal of `NSISFastLib.dll` variants in `%TEMP%`.
4. **Preserve Evidence**
    - Create forensic images of disks and volatile memory for root cause analysis and potential legal/regulatory requirements.

Mid-Term (Systematic Eradication)

1. **Full Host Rebuilds**
    - Given the depth of LOLBIN abuse and registry tampering, a complete OS rebuild of affected systems is strongly recommended.
    - Reinstallation from known-good images is preferable to attempting partial cleaning.
2. **Credential Hygiene**
    - Reset all user and service account passwords associated with compromised systems.
    - Monitor for anomalous authentications post-reset.
3. **Patch and Harden**
    - Ensure all third-party applications (e.g., Google Chrome) and Windows components are fully patched.
    - Disable unnecessary services such as `UI0Detect.exe` in non-critical environments.
4. **Application Control**
    - Enforce AppLocker or equivalent to restrict execution of binaries from `%TEMP%` and `%APPDATA%`.
    - Whitelist only approved update mechanisms for software distribution.

Long-Term (Strategic Defense Improvements)

1. **Behavioral Detection Over Static IoCs**
    - Deploy EDR/XDR platforms capable of identifying DLL injection, LOLBIN abuse, and anomalous registry access.
    - Correlate process activity with outbound network traffic for deeper context.
2. **Network Segmentation**
    - Limit outbound connectivity from user workstations to only required services.
    - Apply SSL/TLS inspection where possible to detect encrypted C2 traffic.

3. **User Awareness & Phishing Defense**
    - Train employees on risks of downloading installers from external collaboration platforms.
    - Enforce safe software acquisition policies.
4. **Compliance Alignment**
    - Map remediation to frameworks such as **NIS2** and **ISO 27001** to ensure legal and regulatory obligations are met.

Ransomwared AI Assessment

The observed campaign is both stealthy and adaptable. Without **rapid containment and long-term strategy**, adversaries could escalate toward **full ransomware deployment**. A layered defense model—covering endpoints, network, identity, and user behavior—is essential to ensuring resilience against this evolving threat.

10. Ransomwared AI Advantage

The investigation highlights not only the sophistication of the malware campaign but also the importance of **advanced detection and contextual intelligence**. Traditional antivirus and signature-based solutions often fail to catch stealthy operations such as **LOLBIN abuse**, **DLL injection**, and **C2 traffic hidden in trusted services**. This is where **Ransomwared AI** provides a decisive advantage.

Early Detection Through Behavioral Analytics

Instead of relying solely on static signatures, Ransomwared AI analyzes behavior in real-time. In this case, the detection was not triggered by the presence of `setup.exe` alone, but by observing:

- Repeated creation and deletion of NSIS DLLs in `%TEMP%`.
- Code injection into `Google\updater.exe`.
- Network communication patterns resembling certificate checks but persisting abnormally.

These behavioral flags allowed Ransomwared AI to recognize malicious activity **even when individual indicators appeared benign**.

Contextual Mapping with MITRE ATT&CK

Ransomwared AI automatically mapped the observed behaviors against the **MITRE ATT&CK framework**, providing defenders with tactical context: execution, persistence, defense evasion, and potential impact. This mapping accelerates analyst response, ensuring that technical findings can be quickly translated into **actionable defensive measures**.

Integrated Threat Intelligence

The system enriched findings with multiple external sandbox results (CAPE, VirusTotal, Zenbox), correlating disparate observations into a unified narrative. This reduced false positives and confirmed that the malware was not isolated but part of a **wider campaign**.

Business-Level Insights

Most importantly, Ransomwared AI provides **executive-ready analysis**. Beyond technical artifacts, the platform delivers assessments of **business impact, compliance exposure, and operational risks**. This ensures leadership can align incident response not only with IT priorities but also with regulatory requirements such as **NIS2, GDPR, and ISO 27001**.

Strategic Value

By identifying the **delivery mechanism** (`flameshot.msi`), the **LOLBIN abuse** (`updater.exe`, `UI0Detect.exe`), and the **network camouflage** (Microsoft/Akamai/Let's Encrypt traffic), Ransomwared AI delivered a comprehensive picture of the threat. This enables defenders to **contain, eradicate, and improve resilience**—not just against this campaign, but against future evolutions of similar attacks.

In conclusion, Ransomwared AI is more than a detection engine: it is a **strategic intelligence platform** that bridges the gap between raw technical signals and high-level business risk management, empowering organizations to stay ahead of ransomware and advanced persistent threats.