Cyber Threat Intelligence Report

Event: blackrock

Generated on: Sat, 19 Jul 2025 19:44:36 GMT

Castle Bravo Project
Open Code. Open Defense. Open Future.

1. Executive Summary

The threat landscape indicates a highly targeted and sophisticated attack against BlackRock's infrastructure. Numerous subdomains and associated IPs of blackrock.com are identified, alongside a significant volume of malicious file hashes. A critical finding is the execution of a file ("software.exe") that drops "dummyTLS" DLLs and temporary files, strongly suggesting a malware infection designed for network manipulation or persistence. The presence of sohu.com domains and related IPs linked to some of the same malicious files points to potential command-and-control (C2) infrastructure, possibly with an origin or target in China. This is indicative of a well-resourced and potentially state-sponsored or financially motivated advanced persistent threat (APT). The potential threat level is Critical. Immediate actions include isolating any systems exhibiting these indicators, deploying all identified file hashes, domains, and IP addresses to all security controls for detection and blocking, and conducting proactive threat hunting across the environment. Furthermore, deep forensic analysis on compromised endpoints is crucial to determine initial access, full malware capabilities, persistence mechanisms, and potential data exfiltration. Enhance network monitoring for all communications to and from the identified IPs and domains, and conduct an urgent review of external and internal vulnerabilities.

2. Actionable Recommendations

Network Forensics:
* Review firewall, proxy, and DNS logs for connections to/from `sohu.com` domains and any IPs associated with identified malicious files.
* Analyze network traffic for unusual TLS activity, self-signed certificates, or non-standard port usage potentially related to `dummyTLS` DLLs.
* Enhance network monitoring for all identified BlackRock subdomains and any associated suspicious IPs.
* Examine VPN and remote access logs for suspicious logins or connections around the time of initial compromise.

Host-Based Analysis:
* Immediately isolate all systems exhibiting indicators of compromise.
* Conduct full forensic images of compromised endpoints for deep analysis.
* Search all endpoints for `software.exe` and any identified malicious file hashes.
* Analyze process execution logs on affected systems for `software.exe` and its child processes, especially those related to network manipulation.
* Locate and analyze `dummyTLS` DLLs and temporary files dropped by `software.exe` to understand their functionality and persistence mechanisms.
* Examine system logs (Event Logs, Registry, MFT) for signs of persistence (e.g., Run keys, Scheduled Tasks, Services) and initial access vectors.
* Assess for evidence of data exfiltration, including large outbound transfers or unusual archive creation.

Intelligence & Threat Hunting:
* Deploy all identified malicious file hashes, `sohu.com` domains, and associated IPs to EDR, SIEM, firewall, and DNS filtering solutions for detection and blocking.
* Proactively hunt across the entire environment for any indicators of compromise, including the presence of `software.exe`, `dummyTLS` components, and network connections to `sohu.com` or other suspicious C2 infrastructure.
* Research `software.exe` and `dummyTLS` in threat intelligence platforms to identify known TTPs, threat actor attribution, and related campaigns.
* Pivot on `sohu.com` domains and associated IPs using OSINT and threat intelligence to uncover additional related infrastructure or threat actor activity.
* Conduct an urgent review of external and internal vulnerability scan results to identify potential initial access points.

3. Attack Timeline (Key Indicators)

1 **MAIN**
`blackrock`

2 **DOMAIN**
`blackrock.com`

3 **FILE**
`27b29394c534b2521c7dafb803674d767ce694e001d7188fe825c51545bf26cd`

4 **PROCESS**
`software.exe`

5 **FILE**
`C:\Users\user\AppData\Roaming\Thinstall\. Torrent\DummyTLS\dummyTLS64.dll (copy)`

6 **FILE**
`C:\Users\user\AppData\Roaming\Thinstall\. Torrent\DummyTLS\dummyTLS.dll (copy)`

7 **FILE**
`C:\Users\user\AppData\Roaming\Thinstall\ Torrent\DummyTLS\-5628.5624.tmp`

8 **IP**
`115.112.241.43`

9 **DOMAIN**
`sohu.com`

4. ATT&CK® Kill Chain

EXECUTION

User Execution: Malicious File

T1204.002

JUSTIFICATION

A file identified by its hash is observed to initiate a process named 'software.exe', indicating that the malicious file was executed.

EVIDENCE

- `27b29394c534b2521c7dafb80367…`
- `software.exe`

PERSISTENCE

Boot or Logon Autostart Executi…

T1547.001

JUSTIFICATION

Malicious files are dropped into the AppData Roaming directory, a common location for establishing persistence through autostart mechanisms.

EVIDENCE

- `C:\Users\user\AppData\Roamin…`
- `C:\Users\user\AppData\Roamin…`
- `C:\Users\user\AppData\Roamin…`

DEFENSE EVASION

Masquerading: Match Legitimat…

T1036.005

JUSTIFICATION

Malicious files are dropped into a path within AppData Roaming that mimics legitimate software or user data, aiming to blend in and avoid detection.

EVIDENCE

- `C:\Users\user\AppData\Roamin…`
- `C:\Users\user\AppData\Roamin…`
- `C:\Users\user\AppData\Roamin…`

COMMAND AND CONTROL

Application Layer Protocol: Web …

T1071.001

JUSTIFICATION

The threat is associated with specific domains and an IP address, which are commonly used by adversaries for command and control communications over web protocols.

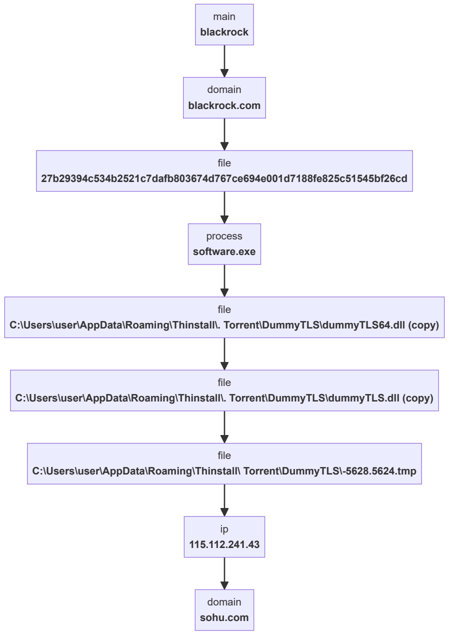
EVIDENCE

- `115.112.241.43`
- `blackrock.com`
- `sohu.com`

5. MITRE ATT&CK® Matrix Overview

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
			User Execution: Malicious File	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder		Masquerading: Match Legitimate Name or Location					Application Layer Protocol: Web Protocols		

6. Attack Flow Diagram


main
blackrock
domain
blackrock.com
file
27b29394c534b2521c7dafb803674d767ce694e001d7188fe825c51545bf26cd
process
software.exe
file
C:\Users\user\AppData\Roaming\Thinstall\. Torrent\DummyTLS\dummyTLS64.dll (copy)
file
C:\Users\user\AppData\Roaming\Thinstall\. Torrent\DummyTLS\dummyTLS.dll (copy)
file
C:\Users\user\AppData\Roaming\Thinstall\ Torrent\DummyTLS\-5628.5624.tmp
ip
115.112.241.43
domain
sohu.com

7. Detailed TTP Analysis

Execution

TA0002

User Execution: Malicious File (T1204.002)

A file identified by its hash is observed to initiate a process named 'software.exe', indicating that the malicious file was executed.

RELATED INDICATORS:

- `27b29394c534b2521c7dafb803674d767ce694e001d7188fe825c51545bf26cd`
- `software.exe`

Persistence

TA0003

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)

Malicious files are dropped into the AppData Roaming directory, a common location for establishing persistence through autostart mechanisms.

RELATED INDICATORS:

- `C:\Users\user\AppData\Roaming\Thinstall\. Torrent\DummyTLS\dummyTLS64.dll (copy)`
- `C:\Users\user\AppData\Roaming\Thinstall\. Torrent\DummyTLS\dummyTLS.dll (copy)`
- `C:\Users\user\AppData\Roaming\Thinstall\ Torrent\DummyTLS\-5628.5624.tmp`

Defense Evasion

TA0005

Masquerading: Match Legitimate Name or Location (T1036.005)

Malicious files are dropped into a path within AppData Roaming that mimics legitimate software or user data, aiming to blend in and avoid detection.

RELATED INDICATORS:

- `C:\Users\user\AppData\Roaming\Thinstall\. Torrent\DummyTLS\dummyTLS64.dll (copy)`
- `C:\Users\user\AppData\Roaming\Thinstall\. Torrent\DummyTLS\dummyTLS.dll (copy)`
- `C:\Users\user\AppData\Roaming\Thinstall\ Torrent\DummyTLS\-5628.5624.tmp`

Command and Control

TA0011

Application Layer Protocol: Web Protocols (T1071.001)

The threat is associated with specific domains and an IP address, which are commonly used by adversaries for command and control communications over web protocols.

RELATED INDICATORS:

- `115.112.241.43`
- `blackrock.com`
- `sohu.com`

Appendix

A.1 YARA Detection Rule ▶

A.2 All Indicators of Compromise (IOCs) ▶

A.3 Data Sources

- **Primary Intel Source:** MISP Event - `blackrock`
- **Sandbox Analysis:** `BR_VirusTotal report for software.exe.pdf`

A.4 Analysis Methodology

This report was generated using the Castle Bravo AI-driven analysis engine. The methodology involves several automated stages: First, structured threat data (e.g., MISP reports) and unstructured data (e.g., sandbox reports) are parsed into a relational graph of indicators. Second, a large language model analyzes this graph to generate a narrative summary, assess threat levels, and identify key indicators. Third, indicators are mapped to the MITRE ATT&CK® framework to contextualize adversary behavior. Finally, derivative artifacts such as attack timelines, YARA rules, and actionable recommendations are produced. The purpose is to rapidly process complex CTI datasets, providing security analysts with a comprehensive and focused head start for manual analysis and incident response.