SECURITY INCIDENT REPORT

Scholomance - APT28 State-Sponsored Attack

TOP SECRET - CLASSIFIED

Incident ID: SCH-2023-APT28
Report Date: November 15, 2023
Classification: **CRITICAL - STATE-SPONSORED ATTACK**
Attribution: **APT28 (GRU - Russian Military Intelligence)**
Impact: Research Data Theft, Credential Compromise, Defense Evasion

Executive Summary

Scholomance experienced a sophisticated, multi-phase cyberattack orchestrated by APT28 (Fancy Bear), a Russian state-sponsored threat group operating under the GRU (Main Intelligence Directorate). The attack involved regulatory compliance-themed phishing, password spraying attacks, malware deployment, and systematic data exfiltration of sensitive research materials.

Critical Impact Assessment

- **28 accounts compromised** via password spraying (405 total attempts)
- **66 malicious files** deployed across 15 hosts
- **12 organizational roles** targeted across magical research divisions
- **LSA Protection disabled** for defense evasion
- **Research data exfiltrated** via staged protect.zip files
- **Attribution confirmed:** APT28 TTPs and infrastructure patterns

RU APT28 Attribution Confirmed

Threat Group: APT28 (Fancy Bear, Sofacy Group)

State Sponsor: Russian Federation - GRU (Main Intelligence Directorate)

Campaign Objectives: Intellectual property theft, research data collection, long-term access establishment

Tactical Characteristics: Compliance-themed social engineering, password spraying, custom malware deployment

Attack Campaign Analysis

Phase 1: Regulatory Compliance Phishing Campaign

APT28 operators initiated the attack using compliance and regulatory themes to establish credibility and urgency:

Malicious Email Infrastructure

- executivecompliance@verizon.com
- executive_compliance@protonmail.com
- executive_compliance@yahoo.com
- compliance.compliance@verizon.com

Social Engineering Subjects

- "[EXTERNAL] Please review your notice now."
- "[EXTERNAL] RE: Please review your notice now."
- "[EXTERNAL] RE:RE: URGENT: Permit needed."
- "[EXTERNAL] You are required to respond or your facility will close."
- "[EXTERNAL] Act now: final notice to your company."
- "[EXTERNAL] IMPORTANT: Provide your information now."

> ### Phase 2: Password Spraying Campaign
>
> **Attack Statistics:**
>
> - **Total Login Attempts:** 405 accounts targeted
> - **IP Addresses Used:** 2,635 unique IPs
> - **Successful Compromises:** 28 accounts
> - **Primary User Agent:** Firefox 69.0
> - **Initial Success:** almcwaters account (173.188.151.49)

Technical Attack Analysis

Malicious Payload Deployment

Following successful credential compromise, APT28 deployed multi-stage malware payloads:

Email Distribution Campaign

- **Sender Addresses:**
  - arunmishra1974@portugalmail.pt
  - ukraine_news@meta.ua
  - str.vidil@meta.ua
- **Campaign Volume:** 69 malicious emails sent
- **File Types:** photo.zip, IOC_30_08.rar, details.zip

Malware Staging Infrastructure

```
# Primary Staging Files C:\ProgramData\66d0975a-e280-46e8-93ef-9f45071c03d2.vbs
C:\ProgramData\dc529177-39b4-4828-8c66-79fe35145d07.cmd C:\ProgramData\dc529177-
39b4-4828-8c66-79fe35145d07.vbs # Credential Collection Tool dc529177-39b4-4828-
8c66-79fe35145d07 (credential harvester) # Database Dump software.save (Windows
database extraction) # Bootloader msedge (persistence mechanism) GUID: aaccd6de-
ce95-4fb2-b2c1-2d7ca08661a3 # Data Staging protect.zip (exfiltration archive)
```

Data Exfiltration

- **Staging File:** protect.zip
- **Destination:** https://webhook.site/dc529177-39b4-4828-8c66-79fe35145d07
- **Method:** HTTPS upload via webhook service
- **Target Data:** Research documents, credentials, system information

Defense Evasion Techniques

- **LSA Protection Disabled:** Local Security Authority protection mechanisms bypassed
- **Security Tool Evasion:** Custom staging locations in ProgramData
- **Legitimate Service Abuse:** Webhook.site for data exfiltration

Compromised Infrastructure

Malicious Domains (25 Total)

Domain	Purpose	File Types
wizard-safety.com	Phishing landing pages	Credential harvesting
wizardregulations.com	Phishing landing pages	Credential harvesting
safetycontrol.com	Phishing landing pages	Credential harvesting
modelinformation.org	Malware hosting	photo.zip
details-model.com	Malware hosting	IOC_30_08.rar
detailsdocuments.org	Malware hosting	IOC_30_08.rar, details.zip
modeldocuments.org	Malware hosting	photo.zip, details.zip

Timeline of Critical Events

October 16, 2023 - 07:48:29 UTC

Initial Compromise: First employee click recorded (Surya Gupta - sugupta)
User Agent: Firefox/47.0
Impact: Credential harvesting page accessed

October 17, 2023 - 01:17:35 UTC

Account Takeover: Second user agent (Firefox/11.0) logs into compromised account
Source IP: 173.188.151.49
Compromised Account: almcwaters
Attack Pattern: Beginning of password spraying campaign

October 2023 (Ongoing)

Mass Password Spraying: 405 accounts targeted across 2,635 IP addresses
Success Rate: 28 accounts compromised
Methodology: Distributed attack to avoid detection

October-November 2023

Malware Deployment Phase: 69 phishing emails sent with malicious attachments
Payload Distribution: photo.zip, IOC_30_08.rar, details.zip
Installation: 66 files deployed across 15 hosts

November 2023 (Recent)

Data Exfiltration: protect.zip archives created and uploaded
Destination: webhook.site exfiltration endpoint
Defense Evasion: LSA Protection disabled on compromised hosts

Targeted Personnel & Roles

Initial Phishing Campaign (8 Roles Targeted)

- Magical Intern
- Magical Quality Control Analyst
- Potion Brewer
- Enchantment Marketing Specialist
- Magical Artifact Seller
- Curse-Breaking Specialist
- Enchantment Researcher
- **Dark Magic Regulation Expert** (4 individuals clicked)

Secondary Malware Campaign (9 Roles Impacted)

- Magical IT Nerd
- Enchantment Marketing Specialist
- Magical Intern
- Lead Research Enchanter
- Magical Artifact Seller
- Curse-Breaking Specialist
- Magical Quality Control Analyst
- Spellcasting Specialist
- Dark Magic Regulation Expert

Surya Gupta (sugupta)

Role: First victim of phishing campaign
Click Time: 2023-10-16T07:48:29.000Z
User Agent: Firefox/47.0
Status: Potential credential compromise

almcwaters

Status: Confirmed compromised account
Takeover IP: 173.188.151.49
Compromise Time: 2023-10-17T01:17:35.000Z
Impact: Used as pivot point for password spraying campaign

APT28 Indicators of Compromise (IOCs)

File Hashes & Malware

Filename	Type	Purpose	Location
details.zip	Malicious Archive	Initial payload delivery	E1TS-LAPTOP (quarantined)
photo.zip	Malicious Archive	Secondary payload	Multiple hosts
IOC_30_08.rar	Malicious Archive	Secondary payload	Multiple hosts
dc529177-39b4-4828-8c66-79fe35145d07.*	Credential Harvester	Credential collection	C:\ProgramData\
software.save	Database Dump	Windows database extraction	Local staging
protect.zip	Exfiltration Archive	Data staging for exfiltration	Multiple hosts

Network Infrastructure

- **Primary Exfiltration:** https://webhook.site/dc529177-39b4-4828-8c66-79fe35145d07
- **Research Target:** https://deathcon-scholomance.io/enclave_secrets/files/important_research.docx
- **Reconnaissance Reference:** https://svch0st.medium.com/active-directory-recon-cheat-sheet-76ccc16dc6e8
- **Tool Download:** https://www.7-zip.org/a/7z2002-x64.exe

Attack Pattern GUIDs

- **Primary GUID:** dc529177-39b4-4828-8c66-79fe35145d07
- **Secondary GUID:** 66d0975a-e280-46e8-93ef-9f45071c03d2
- **Bootloader GUID:** aaccd6de-ce95-4fb2-b2c1-2d7ca08661a3

MITRE ATT&CK Framework Mapping

Tactic	Technique	APT28 Implementation
Initial Access	T1566.001 - Spearphishing Attachment	Compliance-themed emails with malicious archives
Initial Access	T1566.002 - Spearphishing Link	Credential harvesting via fake regulatory sites
Credential Access	T1110.003 - Password Spraying	405 accounts targeted, 28 compromised
Credential Access	T1003 - OS Credential Dumping	dc529177-39b4-4828-8c66-79fe35145d07 tool
Defense Evasion	T1562.001 - Disable Security Tools	LSA Protection disabled
Persistence	T1547.001 - Registry Run Keys	msedge bootloader with GUID
Collection	T1005 - Data from Local System	software.save database extraction
Exfiltration	T1041 - Exfiltration Over C2	webhook.site data upload
Command and Control	T1102 - Web Service	Webhook.site for data exfiltration

Critical Response Actions

IMMEDIATE (0-4 hours)

- **Network Isolation:** Immediately isolate all 15 affected hosts from network
- **Account Security:** Reset passwords for all 28 compromised accounts
- **Domain Blocking:** Block all 25+ malicious domains at network perimeter
- **Webhook Blocking:** Block webhook.site and monitor for data uploads
- **LSA Protection:** Re-enable LSA protection on all Windows systems
- **File Quarantine:** Isolate all instances of photo.zip, IOC_30_08.rar, details.zip

HIGH PRIORITY (4-48 hours)

- **Forensic Analysis:** Image all 15 compromised hosts for detailed analysis
- **Malware Removal:** Remove all staged files from ProgramData directories
- **Credential Audit:** Comprehensive audit of all system and service accounts
- **Research Data Assessment:** Audit access to important_research.docx and related files
- **Threat Intelligence:** Share IOCs with national cybersecurity authorities
- **Backup Verification:** Ensure integrity of all backup systems

STRATEGIC (1-4 weeks)

- **APT28 Hunting:** Comprehensive threat hunt using known APT28 TTPs
- **Security Architecture:** Implement zero-trust principles
- **Email Security:** Enhanced filtering for compliance-themed attacks
- **Password Policies:** Implement anti-spray mechanisms
- **Training Program:** APT28-specific security awareness training
- **International Coordination:** Coordinate with allies on APT28 campaign intelligence

Strategic Assessment

Geopolitical Context

This APT28 operation represents a continuation of Russian state-sponsored cyber espionage activities targeting Western research institutions. The focus on magical research and regulatory compliance suggests intelligence collection objectives aligned with Russian strategic interests in advanced technology sectors.

Attribution Confidence: HIGH

- **Technical Indicators:** GUID patterns consistent with APT28 operations
- **Tactical Alignment:** Password spraying and compliance themes match known APT28 campaigns
- **Infrastructure Patterns:** Domain registration and hosting patterns align with previous APT28 operations
- **Targeting Logic:** Research institution targeting consistent with GRU intelligence priorities

Long-term Implications

- **Intellectual Property Risk:** Potential compromise of proprietary magical research
- **Operational Security:** Need for comprehensive security architecture overhaul
- **International Cooperation:** Intelligence sharing with allied institutions critical
- **Regulatory Compliance:** Enhanced security measures may be required by authorities

Lessons Learned

- **Social Engineering Effectiveness:** Compliance themes highly effective against institutional targets
- **Password Spraying Success:** 6.9% success rate demonstrates vulnerability of account security
- **Defense Evasion Sophistication:** LSA Protection bypass shows advanced technical capabilities
- **Multi-Stage Campaign:** Patient approach over multiple months indicates long-term strategic objectives
- **Research Targeting:** Specific focus on magical research indicates targeted intelligence collection