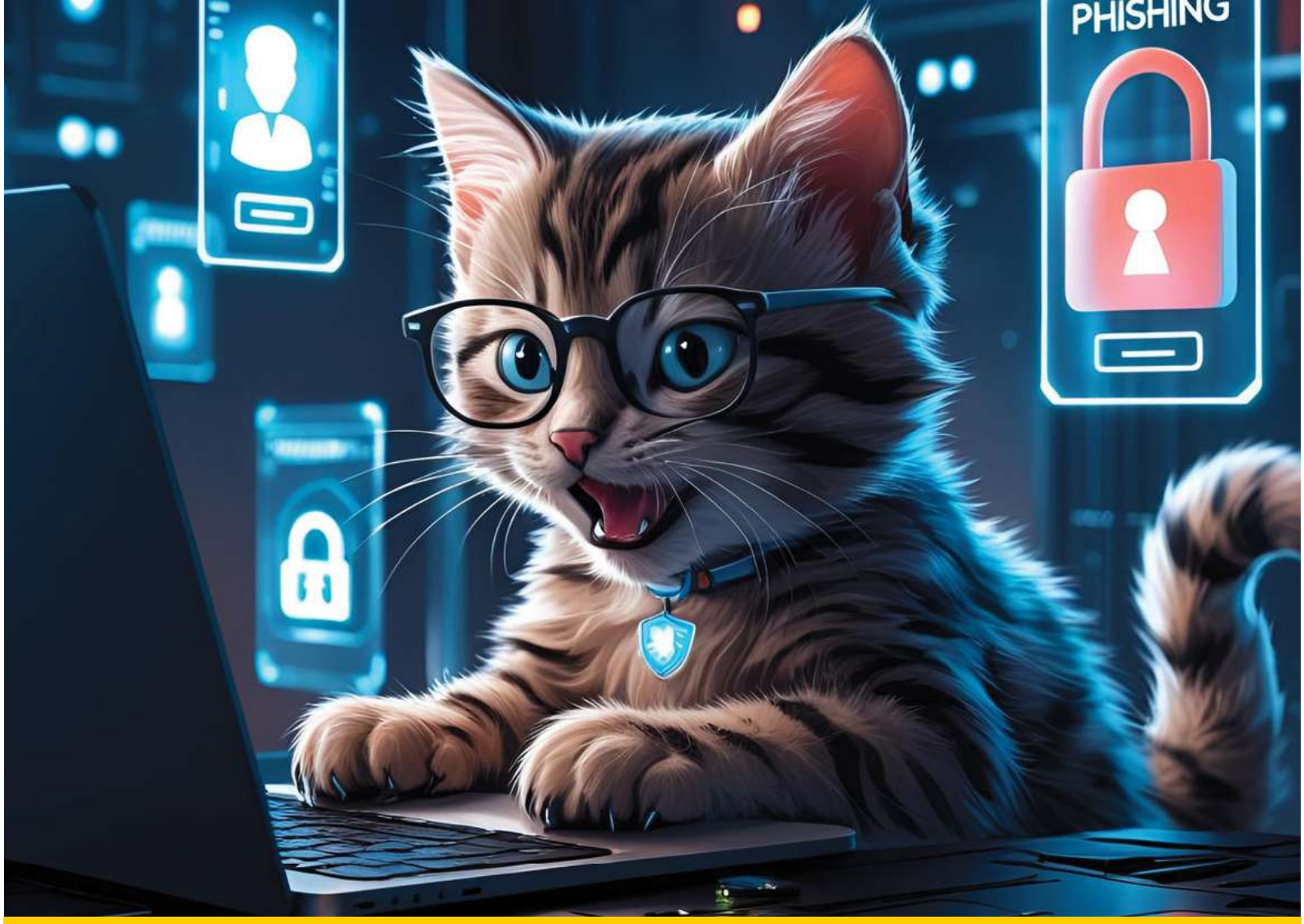
CHARMING KITTEN
APT35

CERTMH_CTI_2025_26

Prepared by **MAHACYBER**

TABLE OF CONTENTS



INTRODUCTION

- **Origin:** 2014
- **Affiliation:** Islamic Revolutionary Guard Corps (IRGC)
- **Aliases:** Newscaster, Parastoo, iKittens, Group 83, NewsBeef, G0058, APT35, PHOSPHORUS, Yellow Garuda, TA453, UNC788, ITG18
- **Key Target Sectors:** Government, Defense, Technology, Military, and Diplomacy
- **Attack Vectors:** Spearphishing, Luring, Social Engineering
- **Attack Region:** North America, Eastern Europe, and the Middle East
- **Malware Used:** BellaCiao, GhostEcho, Hyperscraper, PowerLess, LittleLooter, StoneDrill, MacDownloader
- **Vulnerabilities Exploited:** CVE-2021-44228, Log4Shell (CVE-2021-45046), CVE-2022-47966, CVE-2022-47986, PaperCut bug
- **Tools Used:** BitLocker, DiskCryptor, Fast Reverse Proxy (FRP)

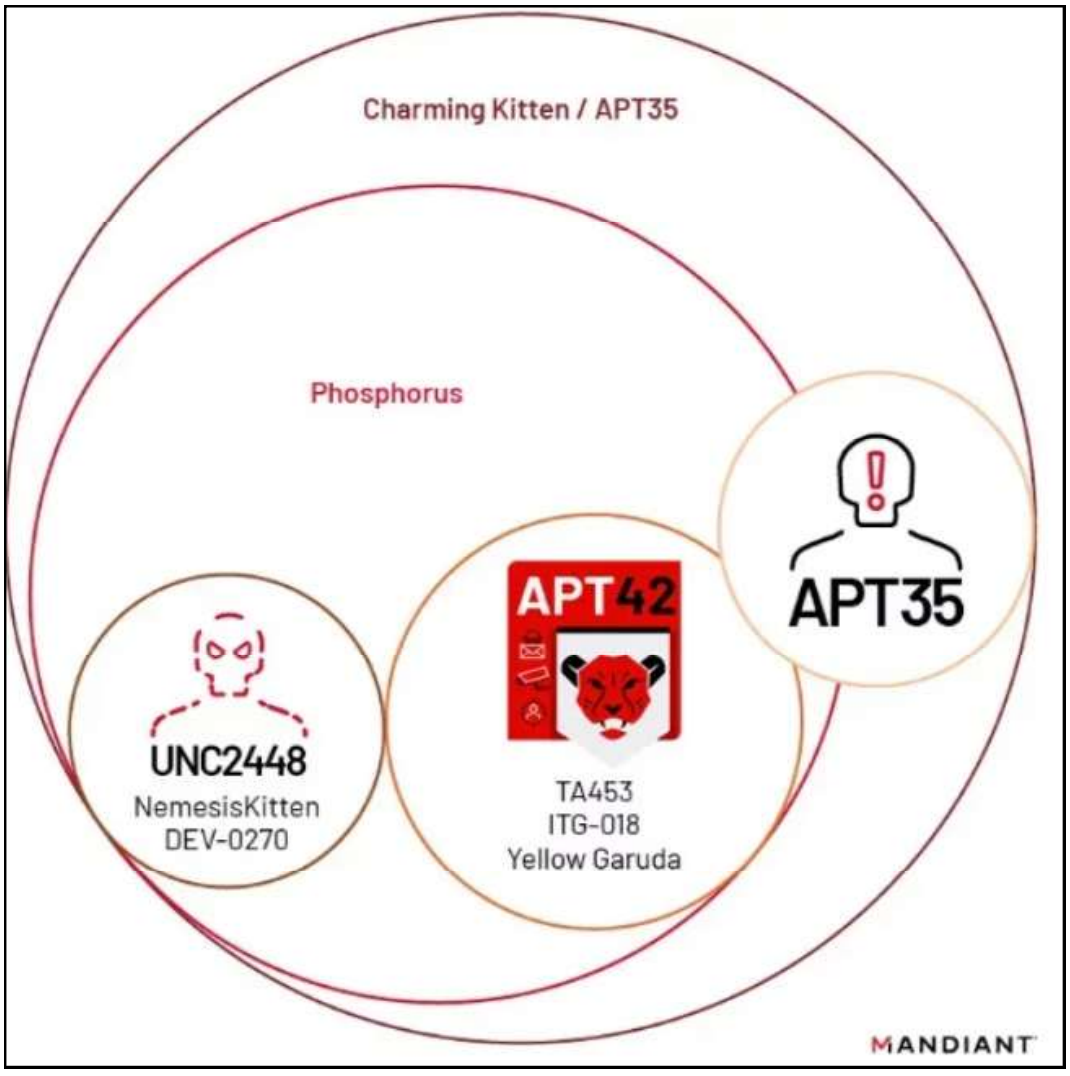
- APT35, also known by various aliases such as Charming Kitten, Phosphorus, and Mint Sandstorm, is an Iranian state-sponsored cyber-espionage group active since at least 2014. The group has been involved in numerous cyber espionage campaigns targeting various sectors globally.

- They have been active since at least 2014 and have been known to target a wide range of sectors and individuals, including biotech, energy, technology, government agencies, journalists, human rights activists, and dissidents. The threat actor has gained attention for their sophisticated and persistent cyber-espionage campaigns.

- In 2019, when APT35's attacks were rampant and it was named behind multiple attacks aimed at several academic institutions in the U.S., France, and the Middle East region, Microsoft took over its infrastructure including 99 domains the attackers used in their malicious campaigns. However, it did not completely break them.

- In 2022 alone, researchers claimed to have documented more than 60 campaigns carried out on behalf of the group. Multiple researchers in a report, pointed at six subgroups of Charming Kitten identified and characterized by their infrastructure, victims targeted, and techniques. These were PHOSPHORUS (being the largest), APT42 (aka Yellow Garuda), NemesisKitten, Tortoiseshell (aka TA453), APT35, TA455 (aka Yellow DEV13), and ImperialKitten

APT35 ALLIANCE



- Multiple aliases to threat groups based on observed activities and characteristics. For instance, MITRE ATT&CK associates APT35 with several other names, including Magic Hound, TA453, COBALT ILLUSION, ITG18, Phosphorus, Newscaster, and Mint Sandstorm.

- This suggests potential overlaps or collaborations between these groups, although the exact nature of their relationships remains a subject of analysis.

- Thus, while APT35 shares certain characteristics and aliases with other Iranian cyber espionage groups, specific distinctions in their targeting and operations suggest they function as separate entities under the broader umbrella of Iran’s state-sponsored cyber activities

Notable Attacks

BellaCPP: New Malware Variant Raises Espionage Stakes

APT35 has deployed BellaCPP, an advanced evolution of its earlier BellaCiao malware. Rewritten in C++ for enhanced speed and stealth, BellaCPP is designed for deep system infiltration, credential theft, and exfiltration of sensitive data—posing serious risks to critical sectors.

Recent operations linked to Charming Kitten include targeted espionage against high-ranking Israeli officials and attempts to disrupt U.S. elections. These campaigns reflect the group's dual focus on intelligence gathering and psychological operations.

🎣**Spreading via Telegram or Webinar**

APT35 has weaponized social engineering, setting up fake academic webinars and exploiting platforms like Telegram to deliver malware and control compromised hosts, showcasing their continued innovation in command-and-control tactics.

🛡️ **Supply Chain and Critical Infrastructure Attacks Intensify**

The NSA and other national security agencies warn of heightened activity by Iranian APTs like Charming Kitten, especially against energy, healthcare, and IT vendors—using third-party compromises to access larger, strategic targets.

Emerging Threat Landscape

- **Iranian nation-state threat actors**: In the near term, Iranian nation-state hackers are likely to leverage targeted attacks, from spear phishing emails aimed at diplomats to destructive wiper malware targeting organizations with ties to U.S. interests.

- **Hacktivists:** It is likely that hacktivists supporting Iran will continue to conduct disruptive attacks and influence operations targeting U.S.-based interests both domestically and abroad. This includes DDoS attacks to disrupt internet access and influence operations on social media platforms.

- **Cybercriminal groups:** These groups could opportunistically exploit global uncertainty to launch phishing campaigns, leveraging world events as a theme for malicious emails and attachments.

- **Other nation-state actors:** There is a potential for other nation-state threat actors to use events to further their interests. These attacks could include false-flag operations where actors from somewhere other than Iran disguise their attacks to appear as if they originated from Iran. This was seen when Russia previously hijacked Iran's cyber infrastructure in 2019 to piggyback into networks already compromised by Iranian actors.

Campaigns & Victims

- *From 2011 till May 2014, Charming Kitten used a dozen of fake personas on social networking sites and ran a wide-spanning cyberespionage operation. It was able to connect to and victimize more than 2,000 individuals across the U.S., the U.K., Saudi Arabia, and Iraq. Link*

- *In December 2017, a member linked with Charming Kitten was accused of hacking HBO's digital content. It claimed that if money was not paid, scripts of television episodes of Game of Thrones would be leaked. Link*

- *In August 2018, an influence campaign targeted the U.S., the U.K., Latin America, and the Middle East. The APT35 group used a network of fake news sites and social media sites to promote anti-Saudi, anti-Israeli, and Pro-Palestine narratives. Link*

- *October 2019, the Charming Kitten employed new spear-phishing methods in a campaign targeting a U.S. presidential candidate, government officials, media persons, and prominent expatriate Iranians. Out of 241 targeted accounts, at least four were compromised. Link*

- *In June 2020, the major U.S. presidential campaigns were targeted by these state-backed hackers. Charming Kitten attempted to target the personnel related to Joe Biden's election campaign. Link*

- *In March 2021, the threat group launched a credential phishing campaign, dubbed BadBlood, that was aimed at senior medical professionals specialized in genetic, neurological, and oncology research in the U.S. and Israel. Link*

- *In January 2022, the APT35 group leveraged Log4Shell (CVE-2021-44228) vulnerability to drop a PowerShell backdoor identified as GhostEcho (aka CharmPower). Link*

- *In mid-2022, the threat group deployed Multi-Persona impersonation social engineering tactics to lure the targeted victims. For instance, to target an individual specialized in Middle Eastern affairs, attackers created the fake persona of Aaron Stein, the director of research at the Foreign Policy Research Institute (FPRI), and Richard Wike, director of global attitudes research at Pew Research Center. Link*

- *In December 2022, the TA453 threat group was observed using a combination of malware, confrontational lures, and compromised accounts to reach a wider set of targets, including politicians, government officials, and researchers. Link*

- *In April 2023, the Charming Kitten was observed using new malware, called BellaCiao, to target users located in the U.S., Turkey, India, Europe, and the Middle East. For initial intrusion, the group exploited known vulnerabilities in internet-exposed applications, including Exchange Server and Zoho ManageEngine. Link*

- *In January 2024, Iranian Cyber Espionage Group Targets Experts on Israel-Hamas War.* Link

- *In February 2024, Iran-Backed Charming Kitten Stages Fake Webinar Platform to Ensnare Targets.* Link

- *In November 2024, an influence campaign targeted the U.S., the U.K., Latin America, and the Middle East. The APT35 group used a network of fake news sites and social media sites to promote anti-Saudi, anti-Israeli, and Pro-Palestine narratives.* Link

Mission Objectives:APT 35's GOALS

Many cybercrimes are linked directly to financial gain, but an allegedly state-sponsored group like Charming Kitten is an exception. It is important to note that the group was tied to the HBO ransomware attack, but that instance is linked to an individual with ties to Charming Kitten and likely was not fully sanctioned by the group. Generally, APT 35 primarily targets organizations and individuals for cyber espionage. These objectives often include:

- **Stealing sensitive information:** This can include intellectual property, government secrets, military plans, or other confidential data.
- **Maintaining long-term access:** APT 35 usually seeks to establish persistent access within target networks, enabling them to gather intelligence over extended periods.
- **Disrupting critical infrastructure:** While less common, some experts believe they may possess the capability for disruptive attacks on critical infrastructure.

Charming Kitten's Common Attack Methods

Charming Kitten isn't generally known for brute force. Instead, they employ a more strategic approach, using a variety of methods to gain access to target systems and steal sensitive information. Here are nine of Charming Kitten's commonly used tactics:

- **Social Engineering:** APT 35 commonly uses sophisticated social engineering techniques, such as fake social media profiles and well-crafted spear-phishing emails to establish connections with targets, gain trust, and compromise accounts.

- **Spear Phishing:** Spear phishing emails are carefully crafted messages that appear to come from legitimate trusted sources. In some cases, the emails even originate from fully legitimate email accounts that have been compromised for this purpose. These emails often contain malicious links or attachments to lure victims into revealing sensitive information or unknowingly download malware onto their systems.

- **Exploiting Known Vulnerabilities:** APT 35 is known for quickly adopting new vulnerabilities such as the Microsoft Exchange Server ProxyShell vulnerabilities and the Log4Shell/Log4j vulnerability.

- **PowerShell-Based Tools:** Charming Kitten commonly uses PowerShell scripts for many of its tools, such as the PowerLess Backdoor. PowerShell is a legitimate scripting language and automation framework built into the Windows operating system, which makes it much easier for the group's tools to blend in with normal system activity and evade traditional security solutions like antivirus.

- **Custom Tool Sets:** APT 35 develops and maintains a set of custom tools for its operations, including backdoors, keyloggers, and information stealers. These tools enable the group to maintain a persistent presence on the target's network, gather sensitive information, and carry out objectives.

- **Multi-Stage Payloads:** APT 35 often uses multi-stage payloads, deploying initial malware components that download and install additional malicious tools onto compromised systems. This helps the group evade detection as initial payloads are often obfuscated or disguised to appear innocent.

- **Malware Loaders:** APT 35 routinely uses malware loaders to deploy other malicious components onto compromised systems, using various techniques to evade antivirus software and other security tools. Once a malware loader has infiltrated a system, they can download and install their custom toolsets.

- **Newscaster:** While no longer in use, it would not be unusual to see this type of tactic used again in the future. Newscaster was a network of fake social media profiles used by Charming Kitten (resulting in the common alias Newscaster Team) for reconnaissance and social engineering. These profiles were used to establish connections with targets, build trust, and compromise accounts to gain access to sensitive data.

APT35 (Charming Kitten) — NIST Framework Mapping

	Activity by APT35	Controls and Recommendations
1	• Spearphish and use social engineering to identify high-value targets. • Gather information about organizations' key stakeholders, credentials, and vulnerable services. • Develop phishing websites, fake profiles, and custom-tailored messages	• Develop and maintain an up-to-date asset inventory. • Perform risk assessments to identify high-risk users, systems, and data. • Implement vulnerability scanning for externally exposed services.
2	• Compromise accounts through phishing or password reuse. • Deploy custom malware and backdoors. • Utilize vulnerable services (Exchange, PaperCut, Log4j) for persistence.	• Provide extensive phish awareness training for users. • Implement Multi-Factor Authentication (MFA). • Apply timely patches and vulnerability fixes. • Implement network segmentation and least privilege controls. • Use application whitelisting and antivirus with behavioral detection
3	• Utilize PowerShell scripting, custom loaders, C2 communications. • Perform credential theft and persistence mechanisms. • Develop methods to avoid antivirus and traditional detections.	• Implement Security Information and Event Management (SIEM) with custom detection rules. • Monitor for suspicious PowerShell activity. • Implement User and Entity Behavior Analytics (UEBA) to identify unusual account behaviors.
4	• APT35 maintains persistence and moves laterally. • Operations may compromise additional accounts or exfiltrate data. • Operations may compromise additional accounts or exfiltrate data.	• Develop and regularly practice incident response plans. • Isolate and cut off compromised endpoints. • Gather and preserve forensic data. • Remove persistence mechanisms and credentials. • Implement containment strategies to limit further spreading.
5	After containment, APT35's persistence mechanisms must be removed and services restored.	• Recover from clean backups. • Reset credentials. • Implement additional acontrols to harden the environment. • Perform post-incident reviews and update incident response plans.

APT35's Techniques

Reconnaissance – Identifying and Profiling Target

APT35 initiates attacks with extensive intelligence gathering:

- Open-Source Intelligence (OSINT): Harvests publicly available data to map organizational hierarchies and identify personnel with privileged access or geopolitical significance.
- Fake Personas & Impersonation: Creates fictitious identities or impersonates legitimate individuals to build rapport with targets.
- Initial Contact Channels: Leverages email, professional networks, and messaging platforms (e.g., LinkedIn, WhatsApp) under the guise of academic or business collaboration.
- Infrastructure Setup: Develops spoofed domains, phishing portals, and cloned websites resembling trusted services to stage future attacks.

Weaponization – Crafting Payloads for Initial Compromise

Upon identifying viable targets, APT35 develops customized payloads:

- Malicious Macros & Remote Templates: Documents embedded with macros or linked to remote templates that drop malware upon opening.
- Credential Harvesting Pages: Fake login portals mimicking email, VPN, or SSO systems to capture credentials.
- Browser Exploits & Cookie Theft: Uses scripts to hijack sessions and steal authentication cookies.
- Anti-Detection Measures: Payloads are obfuscated and employ sandbox evasion techniques to avoid detection by security tools.

Delivery – Transmitting the Payload to the Target
Payloads are delivered through multiple channels to maximize compromise rates:

- Spear-Phishing Emails: Personalized messages referencing current events, research, or security warnings.
- Social Engineering via Messaging Apps: Engages targets over platforms like Telegram or Skype, sharing malicious links or attachments.
- Watering Hole Attacks: Compromises legitimate websites frequented by target groups, injecting malicious code.
- Resilient Infrastructure: Uses frequently rotated domains, encrypted communication, and temporary hosting to evade blacklisting and takedown.

Exploitation – Executing Payloads for Initial Access
After delivery, APT35 payloads exploit vulnerabilities to execute code:

- PowerShell & Scripting Attacks: Executes obfuscated PowerShell scripts to install backdoors and contact C2 servers.
- Zero-Day & N-Day Exploits: Targets unpatched software vulnerabilities in browsers, email clients, or VPNs.
- MFA Bypass Techniques: Uses methods like browser-in-the-middle (BitM) or session token hijacking to bypass multi-factor authentication.

Installation – Gaining Persistence in the Environment
APT35 ensures continued access post-exploitation through various persistence techniques:

- Remote Access Trojans (RATs): Deploys RATs for ongoing surveillance and remote command execution.
- Credential Dumping & Lateral Movement: Utilizes tools like Mimikatz to extract credentials and move laterally across systems.
- Cloud-Based Persistence: Hijacks OAuth tokens and API keys for cloud platforms, maintaining access even after password resets.

Command & Control (C2) – Managing Infected Hosts
APT35 establishes covert communication channels to control infected systems:

- Encrypted C2 Channels: Uses DNS tunneling, HTTPS, and cloud platforms like Google Drive for data exchange.
- Anonymized Platforms: Leverages decentralized services and messaging apps for command delivery.
- Redundant C2 Infrastructure: Employs hardcoded backup domains and fallback mechanisms to ensure persistent connectivity.

Actions on Objectives – Data Theft and Intelligence Gathering
Once access is solidified, APT35 focuses on fulfilling its espionage objectives:

- Data Exfiltration: Steals sensitive emails, research documents, intellectual property, and confidential communications.
- Surveillance Activities: Implements keyloggers, screen recorders, and monitoring tools to track user behavior.
- Account Hijacking & Further Phishing: Uses compromised accounts to escalate campaigns or deceive additional victims.
- Stealthy Exfiltration: Data is exfiltrated through encrypted archives or stealthily uploaded to cloud services to avoid detection.

MITRE ATT&CK

Tactic	Technique	ID
Reconnaissance	Spearphishing for Information	T1598.002
	Gather Victim Identity Information	T1589
Resource Development	Compromise Infrastructure	T1584
Initial Access	Spearphishing Link	T1566.002
	Spearphishing Attachment	T1566.001
	Drive-by Compromise	T1189
Execution	User Execution: Malicious Link	T1204.001
Persistence	Web Shell	T1505.003
	Account Manipulation	T1098
Privilege Escalation	Exploitation for Privilege Escalation	T1068
Defense Evasion	Obfuscated Files or Information	T1027
	Indicator Removal on Host	T1070
Credential Access	Credential Dumping	T1003
	Input Capture: Keylogging	T1056.001
Discovery	System Information Discovery	T1082
	Account Discovery	T1087
Lateral Movement	Remote Services: SSH	T1021.004
Command and Control	Web Service C2	T1102
	Application Layer Protocol	T1071
Exfiltration	Exfiltration Over Web	T1041

Recommendations & Conclusion

Charming Kitten's deployment of BellaCPP is a stark reminder of the ever-evolving cyber threat landscape. Organizations must remain proactive, investing in robust cybersecurity measures and fostering industry collaboration. By doing so, we can reduce the impact of state-sponsored APTs and ensure a safer digital environment for all.

- **Strengthen Phishing and Social Engineering Defenses**
  – Conduct regular user awareness training, phishing simulations, and enforce email filtering solutions.

- **Enforce Strong Authentication and Access Controls**
  – Implement phishing-resistant MFA (e.g., FIDO2/WebAuthn) and enforce least privilege principles.

- **Patch Vulnerabilities and Secure Public-Facing Infrastructure**
  – Maintain a strict patch management program and continuously monitor exposed assets.

- **Monitor for Indicators of Compromise (IOCs) and Threat Actor Tactics (TTPs)**
  – Use SIEM, threat intel feeds, and automated IOC matching to identify suspicious activity.

- **Secure Third-Party Access and Supply Chains**
  – Conduct regular vendor risk assessments, enforce VPN/MFA, and limit third-party privileges.

- **Develop and Test Incident Response Plans**
  – Include APT simulation scenarios and tabletop exercises for advanced threat response.

- **Restrict and Monitor PowerShell and Script Execution**
  – Apply constrained language mode, log PowerShell activity (event ID 4104), and block unsigned scripts.

- **Simulate Attacks via Red Teaming and Purple Teaming**
  – Test detection and response against TTPs from APT35 using tools like Caldera or Atomic Red Team.

- **Isolate and Monitor High-Value Targets**
  – Provide enhanced security controls and continuous monitoring for VIPs and privileged users.

- **Secure Cloud Environments**
  – Enforce MFA, audit OAuth/API access, and monitor for anomalous activity via CASB tools.

- **Implement Threat Hunting and Behavioral Detection**
  – Proactively search for stealthy APT behavior using UEBA, EDR telemetry, and threat hunting playbooks.

Indicator of Compromise (IOC)

IOC	Type
theworkpc[.]com	Domain
instagram-com[.]site	Domain
28332bdbfaeb8333dad5ada3c10819a1a015db9106d5e8a74beaaf03797511aa	Hash-256
d30abec551b0fb512dc2c327eeca3c43	Hash
34d37f64613f3fe00086ac8d5972db89	Hash
28de2ccff30a4f198670b66b6f9a0ce5f5f9b7f889c2f5e6a4e365dea1c89d53	Hash-256
78e4975dc56e62226f4c56850efb452b	Hash
5d3ff202f20af915863eee45916412a271bae1ea3a0e20988309c16723ce4da5	Hash-256
90e5fa3f382c5b15a85484c17c15338a6c8dbc2b0ca4fb73c521892bd853f226	Hash-256
e8f50ecea1a986b4f8b00836f7f00968a6ecba4f	Hash
75b7db0597f234838e7c8431b57870411842775d	Hash
3b9a2e34f5d603b55cf7fd223d4e5c784b805242	Hash
2374f5a9278b209563e8193847a76c25c12eec8f	Hash
c45bffb5fe7056075b966608e6b6bf82102f722b5c5d8a9c55631e155819d995	Hash-256
66d36d0b170cf1a0001cca16357961a2f28cba60	Hash
1504da49f6fe8638c7e39d4bcb547fbb15376462	Hash
9b7b29af74d5d2d3cb4cace1ebf2602c345e6cc299da1c18ca506eda201698d9	Hash-256
186f07279ac0f15cc7be5caf68addabb2091bc84	Hash
b66ae149bbdfc7ec6875f59ec9f4a5ae1756f8ba	Hash
448e6d519a340845a55b4b1809488427c0d79cdd	Hash
08d2aea84d6c148ff2ad4653856fb080eb99abf2	Hash
41b37de3256a5d1577bbed4a04a61bd7bc119258266d2b8f10a9bb7ae7c0d4ec	Hash - 256
9410963ede9702e7b74b4057fee952250ded09f85a4bb477d45a64f2352ec811	Hash - 256
c2c1d804aeed1913f858df48bf89a58b1f9819d7276a70b50785cf91c9d34083	Hash - 256
69eb4fca412201039105d862d5f2bf12085d41cb18a93398afef0be8dfb9c229	Hash - 256
afd06652b24811d7e03d5525b292293dbdf49b8c0e450d748cab0289aecdbc02	Hash - 256

a485ef522a00edc7eb141f4ef982dd52b3e784ea8d8f1bb0ca044a61ce642eac	Hash - 256
4bcc2ad5b577954a6bd23aff16566ce0784a71f9526a5ae849347ae766f4033f	Hash - 256
21c5661eb5e54d537c6c9394d7bd4accf53e06851978a36c94b649c4f404a42e	Hash - 256
110c77f66a8d4d8ccc9dc468744302cf368efd071e3e4af39338b699f6bc7808	Hash - 256
2c33b1dd793ad5e59180719d078301ee7ebb6cf7465286c19b042accca6ac749	Hash - 256
003676e6240421426e5c0919eb40bdde52b383eb1c54596deb77218c3885cdc5	Hash - 256
c1664df788f690fd061994ed3eb9d767e2f293448ce9d7ff5bff37549e9e4dab	Hash - 256
5ee98a677f58b897df3287448e63a1a781d312d2a951f438e1d7e4ab658fa4a0	Hash - 256
7eb564f0afc23cc8186e67f8c0d7e6c80215b75c9f0c4b35f558a9e35743ca41	Hash - 256
33a61ff123713da26f45b399a9828e29ad25fbda7e8994c954d714375ef92156	Hash
162[.]216[.]242[.]208	IP
202[.]108[.]8[.]82	IP

Reference

- https://socradar.io/apt-profile-who-is-phosphorus/
- https://www.ts-way.com/it/risorse/2024/09/12/charming-kitten-e-il-cyberspionaggio-iraniano/
- https://www.stamus-networks.com/blog/the-hidden-claws-of-apt-35-charming-kitten
- Iranian APT Group "Charming Kitten" Deploys New Malware: What You Need to Know