TLP:CLEAR

Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

JPCERT CC®

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

警察庁
National Police Agency

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

National Cyber Security Centre
a part of GCHQ

Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society

Publication: May 14, 2024

TLP:CLEAR

Executive Summary

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the following organizations (hereafter referred to as the "authoring agencies") have written and coauthored this guidance, in coordination with key government, non-government, industry, and civil society partners. The authoring agencies are releasing this joint guidance to provide cybersecurity guidance to high-risk community (HRC) entities such as civil society organizations and individuals:

- Department of Homeland Security – Office of Intelligence and Analysis (DHS I&A)
- Federal Bureau of Investigation (FBI)
- Canadian Centre for Cyber Security (Cyber Centre) (CCCS)
- Estonian National Cyber Security Centre (NCSC-EE)
- Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
- National Center of Incident Readiness and Strategy for Cybersecurity (NISC) Japan
- National Cyber Security Centre – Finland (NCSC-FI)
- National Police Agency (NPA) Japan
- United Kingdom National Cyber Security Centre (NCSC-UK)

Civil society—nonprofit, advocacy, cultural, faith-based, academic, think tanks, journalist, dissident, and diaspora organizations, communities, and individuals involved in defending human rights and advancing democracy—are considered high-risk communities. Often, these organizations and their employees are targeted by state-sponsored threat actors who seek to undermine democratic values and interests. Regularly conducted as a type of transnational repression (also referred to as digital transnational repression), state-sponsored actors compromise organizational or personal devices and networks to intimidate, silence, coerce, harass, or harm civil society organizations and individuals.

According to industry reporting, state-sponsored targeting of high-risk communities predominantly emanates from the governments of Russia, China, Iran, and North Korea. Actors typically perform extensive pre-operational research to learn about potential victims, gather information to support social engineering, or obtain login credentials. Actors target organization networks or personal accounts (e.g., email) and devices of individuals for surveillance and monitoring, often via spyware applications—malicious software that collects data from affected devices.

This guide provides recommendations for civil society organizations and individuals to mitigate the threat of state-sponsored cyber operations based on observed malicious behavior. The guide also provides recommendations for software manufacturers to improve the security posture of their customers.

Table of Contents

Introduction

Industry reporting emphasizes the prevalence and global nature of cyber threats to civil society, necessitating their preparedness against a diverse range of politically and ideologically motivated threat actors. Civil society organizations are considered high-risk communities (HRC) due to their high threat level and low defense capacity. Specifically:

- Civil society organizations and their staff are at ***high threat*** of being targeted by malicious cyber actors. Based on industry reporting, these organizations and their staff are known targets as state-actors may seek to undermine democratic values.
- Civil society organizations often have ***low defense capacity***. These organizations lack internal IT support and essential cyber hygiene to prevent the possibility of malicious activity (e.g., lifecycle management, patch management, multifactor authentication, password management). Individuals that fall under the civil society umbrella often rely on insecure channels for communication and need to manage public profiles to advance their work. Organizations with low defense capacity are ill-prepared for and vulnerable to common cyber threats, such as social engineering attempts.

Low defense capacity is exacerbated, in most cases, by products and services designed in a manner that places the burden of reducing cyber threats on the customer or end user. For example, the customer or end user is required to take specific, sometimes onerous, actions to improve their cyber posture.

This joint guide, developed as part of CISA's High-Risk Community Protection (HRCP) initiative* and NCSC-UK's Defending Democracy campaign†, provides mitigation measures for civil society organizations to reduce their risk based on common cyber threats. The authoring agencies strongly encourage civil society organizations and affiliated individuals to apply the mitigations provided in this joint guide. The authoring agencies also encourage software manufacturers to take responsibility for their customers' security outcomes by applying the mitigations in this advisory and designing products that prevent the most common classes of attack by malicious actors.‡

* Established in 2023, CISA's HRCP initiative serves as the enduring home for the agency's work to identify and partner with high-risk communities to understand the threats they face, identify the resources which can bolster their defense, and close gaps in support. For information on CISA's HRCP, see Department of Homeland Security Press Release Secretary Mayorkas Discusses New U.S. Efforts to Counter Spread of Digital Authoritarianism at Summit for Democracy.

† NCSC-UK takes a whole of society approach to cyber defense and views civil society as one of three sectors of focus for their work. Through the NCSC's Defending Democracy work, the NCSC is seeking to partner with high-risk public and elected officials to advance understanding of the sophisticated threats targeting individuals across personal and enterprise devices. For more information, see NCSC-UK's webpage Defending Democracy.

‡ Products designed with security and safety in mind are referred to as "secure by design." A key tenant of secure by design is that software manufacturers take ownership of their customers' security outcomes by building cybersecurity into design and development. For more information on secure by design, see cisa.gov/securebydesign and joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default.

Cyber Threats to Civil Society

The lack of reporting in threat telemetry and intelligence feeds, coupled with HRCs' limited accessibility to enterprise-level solutions, hinders commercial and government organizations' accurate measurement of threats posed to HRCs. However, industry reporting indicates a consistent pattern of state-sponsored cyber actors targeting specific segments of civil society. Notably and frequently non-governmental organizations (NGOs), think tanks, human rights activists, and journalists are targeted by state-sponsored actors:

- According to Microsoft, in 2023 NGOs and think tanks were the second highest targets of state-sponsored actors (following the Information Technology Sector).[1]
- As of November 2023, CrowdStrike reporting revealed that five state-sponsored groups are known to target think tanks,[2] eleven groups represent potential threats to NGOs,[3] two groups target dissidents,[4] and one group is known to target nonprofit organizations (NPOs).[5]
- Cloudflare has observed that malicious cyber activity against civil society organizations is "generally increasing."[6] In Quarter 2 of 2023, NPOs were targeted more than any other industry when looking at malicious traffic to NPO websites as a proportion of total traffic.[7] In Quarter 3 of 2023, NPO and independent media organizations placed second behind the metals and mining industry, with 17.14% of all traffic to NPOs representing distributed denial-of-service (DDoS) attacks.[8] Similarly, the European Union Agency for Cybersecurity (ENISA) found that targeted individuals within civil society were the second most-targeted sector globally between July 2022 and June 2023.[9]

State-sponsored actors target civil society organizations and their staff as part of their toolkit to undermine democratic values. Specifically, they target organizations and individuals online primarily as a means of intimidation, harassment,§ coercion, and surveillance—a type of transnational repression called digital transnational repression.

Digital transnational repression is often preceded by extensive online research of corporate websites, social media pages, geopolitical publications, and press releases so actors can gather information on target organizations and individuals. After research, state-sponsored actors will often gain access to organization networks or personal devices via (a) social engineering that lures victims to divulge account credentials or download malware or (b) having users download seemingly legitimate apps that house malicious software. After gaining access to devices, actors often install spyware on the devices. Spyware is a commercial tool that provides extensive surveillance capabilities, including location tracking, image and audio capture, and access to personal files and communications.

For more information on the state-sponsored groups known to target civil society organizations, see Appendix A: State-Sponsored Actors. For technical information on cyber operations that enable actors to gain access to networks and devices and surveil and monitor individuals, see Appendix B: State-Sponsored Actors' Tactics and Techniques.

§ Harassment, as an independent tool, is deployed by states to silence, control, or suppress dissidents, and digital harassment is when this occurs online, for example via mobilizing social media accounts against individuals.

Mitigations

Civil Society Organizations

The authoring agencies strongly encourage civil society organizations to implement best practices as defined by CISA's Cross-Sector Cybersecurity Performance Goals (CPGs). These cybersecurity controls provide a minimum set of practices and protections that are informed by the most common and impactful threats and behaviors. To mitigate state-sponsored actors performing reconnaissance and gaining initial access to enterprise networks via phishing and compromised credentials, prioritize the following:

KEY CHARACTERISTICS OF THE CPGs:

- A prioritized subset of cybersecurity practices.
- Prioritized for risk reduction.
- Informed by threats observed by CISA and its government and industry partners.
- Intended to meaningfully reduce risks to both critical infrastructure operations and the public.

1) **Keep software updated on user devices and IT infrastructure.** Software updates fix known flaws. Installing them promptly means actors cannot leverage these flaws to access systems.
2) **Implement phishing-resistant multifactor authentication (MFA)** [CPG 2.H]. Set up phishing-resistant MFA makes it more difficult for actors to compromise user accounts, and often make legitimate user sign-ins simpler at the same time. See CISA's Phishing-Resistant Multifactor Authentication guide for additional information.
3) **Audit accounts and disable unused and unnecessary accounts.** Remove needless accounts to reduce access vectors that actors can use to get into the system.
4) **Disable user accounts and access to organizational resources for departing staff** [CPG 2.D]. Disablement of accounts can minimize exposure of the system, removing options actors can leverage for entry into the system.
5) **Apply the Principle of Least Privilege.** Audit accounts with extensive or high-impact permissions (admin access) and remove any unnecessary permissions to reduce the damage that an actor can inflict through a compromised an account. Avoid using admin user accounts for regular daily tasks [CPG 2.E]. Usage of admin user accounts should be regularly monitored to detect unauthorized and malicious activity.
6) **Exercise due diligence when selecting vendors, including cloud service providers (CSP) and managed service provider (MSPs).** This reduces supply chain risks. Use only reputable vendors that verbalize how they embrace Secure by Design practices. See the Software Manufacturers section for CISA's Secure by Design Pledge and recommended practices.
7) **Review contractual relationships** with all service providers, prioritizing providers of critical services first. Ensure contracts include:
   - Security controls tailored to meet the specific needs of the customers;
   - Appropriate monitoring and logging of provider-managed customer systems;
   - Continuous monitoring of the service provider's presence, activities, and connections to the customer network, ensuring compliance with cybersecurity performance objectives and Secure by Design principles; and
   - Notification of confirmed or suspected security events and incidents occurring on the provider's infrastructure and administrative network to an up-to-date recipient.

8) **Manage architecture risks** by:
   - Auditing and reviewing connections between customer systems, service provider systems, and other client enclaves; particularly those exposed to the internet, such as cloud services, email servers and virtual private network (VPN) servers.
   - Using a dedicated VPN to connect to MSP infrastructure; all network traffic from the MSP should only traverse this dedicated secure connection.
9) **Implement basic cybersecurity training** to cover concepts such as account phishing, email and web browsing security, and password security [CPG 2.I]. Ensure training addresses state-sponsored cyber actor targeting of personal emails and devices, and that staff should protect their personal emails accounts and mobile devices from compromise by applying the recommendations to individuals below.
10) **Develop and exercise incident response and recovery plans** [CPG 2.S]**.** Ensure plans cover at least the systems that are critical and important to the organization and include who to contact or report the incident to for assistance. See the Contact Information section of this guide for reporting information of the applicable authoring agency. See the Resources section for guidance on creating incident response and recovery plans.

Civil Society Individuals

The authoring agencies strongly encourage civil society individuals to implement the following recommendations to mitigate the impact of state-sponsored actors gaining access to corporate networks, as well as mobile devices, for surveillance and monitoring. These mitigations align to CISA's Project Upskill. Project Upskill, developed as part of CISA's Joint Cyber Defense Collaborative's (JCDC's) 2023 High Risk Communities Protection planning effort, is a series of guides to help non-technical users enhance their digital security. See Project Upskill for details and guidance on how to implement the following recommendations.

- **Use strong passwords on accounts and implement MFA** [Project Upskill, Module 2, Topic 2.0, Topic 2.2]
  - **Use robust MFA solutions,** such as digital or hardware tokens, to safeguard accounts.
- **Limit exposure of publicly available information**.
  - **Exercise caution on social media** and online. Be mindful of the information you are inputting onto public-facing platforms.
  - **Advocate limiting data shared among friends and family**, enhancing overall security against potential exploitation.
- **Verify contacts and be aware of social engineering**. To enhance personal and organizational cybersecurity, comprehension of the specific threats and behaviors relevant to your industry or self is essential. Establish a reference list that outlines potential threats, considering the unique risk landscape associated with your work, interests, and organizations. This can include industry-specific cyber threats, regulatory considerations, and historical attack patterns.
  - **Confirm identities of social media contacts** to mitigate the risk of fake profiles and social engineering tactics.
  - **Stay vigilant against impersonation attempts**, especially from individuals claiming to be journalists or other personas.

  - **Be cautious when clicking on links or attachments** in emails, text messages, or other communications platforms.
  - **Exercise caution when clicking on links or attachments from unknown sources**.
- **Use encryption measures to protect all communications when interacting with online services** [Project Upskill, Module 4, Topic 4.0]. Encryption is vital to safeguarding all communications when engaging with online services. Without encryption, threat actors can exploit unencrypted or unauthenticated channels to inject malware into user devices, posing significant risks to privacy and security. To mitigate these risks, users should prioritize accessing websites and services over HTTPS, which encrypts the data exchanged between the user's device and the website's server—thereby protecting against eavesdropping and tampering by malicious actors. Additionally, utilizing encrypted messaging apps further enhances security by ensuring that messages and calls remain intact, confidential, and inaccessible to unauthorized parties.
- **Select apps carefully.**
  - **Use trusted app stores** to avoid potential threats from malicious third-party applications.
  - **Thoroughly check app details and developer information** before downloading, thus mitigating potential risks at the source.
  - **Vet third-party apps**, ensuring they meet cybersecurity standards [Project Upskill, Module 1, Topic 1.4].
- **Regularly review and restrict app permissions** to minimize data exposure, which will enhance overall security [Project Upskill, Module 1, Topic 1.3].
- **Keep applications and OS updated** [Project Upskill, Module 1, Topic 1.1].
  - **Install updates promptly** to prevent exploitation of vulnerabilities by threat actors.
  - **Enable automatic OS and app updates** for proactive security maintenance.
- **Consider rebooting your mobile device weekly** to potentially eliminate installed spyware. Some mobile devices provide the capability to schedule reboots, enabling you to set them at a designated time, with scheduling options ranging from daily to weekly intervals.
- **Secure browsing habits and digital footprint management.**
  - For iPhones/iPads, **enable iOS Private Wi-Fi Address**. In a high-risk target environment, consider activation of the **iOS Lockdown Mode**. For more information on iOS Lockdown Mode, visit the Apple Support - About Lockdown Mode webpage.
  - **Consider employing remote browser isolation solutions** for enhanced web browsing security during sensitive research.
  - **Use a standard user account for browsing and other regular tasks** [Project Upskill, Module 1, Topic 1.0].

Software Manufacturers

The authoring agencies strongly encourage software manufacturers to publicly commit to and actively implement the Secure by Design Pledge. This commitment entails embracing Secure by Design principles, including (1) assuming accountability for customer security outcomes, (2) embrace radical transparency and unwavering accountability, and (3) lead from the top and implement top-down leadership to drive transformative changes aimed at prioritizing security at every stage of software development and deployment. Mitigations to improve the security posture of their customers include:

- **Vulnerability management. Working to eliminate entire classes of vulnerability in their products** to reduce the opportunity for compromise. Malicious cyber actors often exploit well-known weaknesses in software to deliver their payloads via malware. Manufacturers should work to eliminate these classes of vulnerability in their products to prevent compromise.
- **Enabling MFA by default in all products**.
- **Provide logging at no additional charge to the customer, and alert customer**s of suspicious or anomalous behavior on their networks.
- **Implement attention grabbing alerts so customers are aware of unsafe configurations**, suspicious behavior, and when they are downloading malware.
- **Include details of a Secure by Design program in corporate financial reports.**

Contact Information

U.S. organizations: To report suspicious or criminal activity related to information found in this guide, contact:

- CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870 or your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

Canadian organizations: Report incidents by emailing CCCS at contact@cyber.gc.ca

Estonian organizations: Report cyber security incidents to cert@cert.ee or call +372 663 0299.

Finnish organizations: Contact NCSC-FI by emailing at ncsc@ncsc.fi or report incidents to https://www.kyberturvallisuuskeskus.fi/en/report

Japanese organizations: To report incidents related to this guidance, please visit https://www.kantei.go.jp/jp/forms/nisc_opinion.html (NISC) or send an email to info@jpcert.or.jp (JPCERT/CC), and to report criminal activity, please visit https://www.npa.go.jp/bureau/cyber/soudan.html (NPA).

United Kingdom organizations: Report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

Resources

See CISA's Project Upskill for detailed guidance on how to improve your cybersecurity posture and raise the cost, in terms of time and resources, for a threat actor to target you.

See CISA's Cybersecurity Training & Exercises webpage for cybersecurity training to the available to the general public.

For more information on incident response and recovery plans, see:

- CISA: Incident Response Plan Basics and Federal Government Cybersecurity Incident and Vulnerability Response Playbook. (Although tailored to U.S. Federal Civilian Branch (FCEB) agencies, these playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail steps for both incident and vulnerability response.)
- NCSC-EE: For cyber security awareness and prevention, please visit https://www.ivaatlik.ee/

Access Now's Digital Security Helpline and Amnesty International's Security Lab for hands-on support to human rights defenders and members of civil society. Email Cisco for assistance at no-spyware@external.cisco.com.

If you are experiencing a digital emergency, Access Now's Digital Security Helpline and Amnesty International's Security Lab offer hands-on support to human rights defenders and members of civil society who believe they are the subject of a targeted attack.

If you believe you have been targeted with spyware, you can also send an email to Cisco for assistance at no-spyware@external.cisco.com for investigation.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies.

Acknowledgments

Atlantic Council, Authentic8, Cisco Talos, Cloudflare, and Meta contributed to this guide.

Appendix A: State-Sponsored Actors

According to industry reporting, state-sponsored targeting of HRCs predominantly emanates from the governments of Russia, China, Iran, and North Korea; ** However, think tank research suggests that numerous other countries also leverage digital transnational repression tactics, focusing on punishing and silencing dissenters.

Groups known to target civil society organizations include the following:

- **Velvet Chollima**: A group linked to the Democratic People's Republic of Korea (DPRK) that conducts cyber espionage. Velvet Chollima primarily targets journalists reporting on Korean Peninsula matters and researchers concentrating on East Asian policy within NGOs, think tanks, and academic institutions.[10]
    - **Aliases**: Kimsuky, THALLIUM, Black Banshee, Emerald Street
- **Mustang Panda**: A group affiliated with PRC that focuses on political espionage. The group extensively targets NGOs, religious institutions, think tanks, and activist groups across diverse geographic locations, including the United States, Europe, Taiwan, Hong Kong, Tibet, Myanmar, Mongolia, Vietnam, Afghanistan, Pakistan, India, and others. Their principal aim revolves around the meticulous surveillance of victim activities coupled with the deliberate endeavor to tarnish and impugn their reputations. [11] Mustang Panda's tactics underscore its effectiveness in executing targeted and prolonged political espionage campaigns.
    - **Aliases**: BRONZE PRESIDENT, TA416, RedDelta
- **Charming Kitten**: A group associated with the government of Iran that specializes in targeting political dissidents, human rights organizations, media outlets, and scholars engaged in Iranian studies to extract intelligence through cyber espionage. According to CERTFA, a Computer Emergency Response Team that specializes in tracking Iranian cyber threat actors, Charming Kitten has been observed targeting "individuals, academics, journalists, activists, think tanks, military and government sectors in the United States, Europe, and the Middle East since as early as 2014."[12] Between August 2020 and May 2021, IBM X-Force documented Charming Kitten's successful compromise of multiple victims within the Iranian reformist movement. This campaign strategically focused on infiltrating personal webmail and social media accounts, aligning with surveillance objectives leading up to the June 2021 presidential elections in Iran.[13]
    - **Aliases**: TA453, COBALT ILLUSION, Magic Hound, ITG18, Phosphorus, Newscaster, APT35, Mint Sandstorm
- **Earth Empusa**: Identified as a PRC state-sponsored group whose primary focus is surveilling activists, journalists, and dissidents, particularly among Uyghurs residing abroad in countries such as Turkey, Kazakhstan, the United States, Syria, and Australia. [14]
    - **Aliases**: POISON CARP[15], Evil Eye[16]

** Industry and government track activity clusters using various analytic methodologies; they identify activity deemed to be coming from the same group of actors by giving the group a name. Some groups have multiple names or partially overlap because organizations may track activity independently. The term advanced persistent threat (APT) is generally used for well-resourced, state-sponsored groups that engage in sophisticated activity often targeted and aimed at prolonged network/system intrusion. For more information, see CISA's webpage on nation-state cyber actors and attack.mitre.org/groups.

- **Syrian Electronic Army (SEA) or APT-C-27**: A group focused on executing targeted operations against humanitarian organizations, journalists, and dissidents, notably those affiliated with the anti-regime Free Syrian Army.[17]

Appendix B: State-Sponsored Actors Tactics and Techniques

For the authoring agencies, understanding the behavior of malicious cyber actors is often the first step to protect networks and data. For well-resourced organizations, the success network defenders have in detecting and mitigating malicious cyber operations depends on this understanding. Although civil society organizations may lack internal network defense staff, understanding malicious behaviors will enable them to make informed resourcing decisions on basic cybersecurity controls to mitigate state-sponsored activity.

This appendix provides an overview of cyber operations that enable actors to gather information in support of future targeting, and then gain access to enterprise networks or mobile devices in support of surveillance and monitoring or to learn about the target's mission, interests, and contacts. Activity is mapped to the MITRE ATT&CK Framework, a globally accessible knowledge base of malicious cyber behaviors, where behavior is categorized into defined tactics and techniques††:

- **Tactics** represent the "why"—in other words, malicious cyber actors' technical objectives, end goals, and motive(s) for performing their actions.
- **Techniques** represent "how" an adversary achieves a tactical goal by performing an action.

MITRE ATT&CK is organized into three "technology domains" frameworks, or the ecosystem within which actors operate: Enterprise, Mobile, and Industrial Control Systems.‡‡ This appendix provides an overview of tactics and techniques against civil society organizations for the Enterprise and Mobile frameworks, version 14.

Enterprise

Tactic: Reconnaissance [TA0043]

Definition: Cyber actors gather information they can use in future operations.

Description of Known Reconnaissance Techniques: State-sponsored actors use open-source research to gather information, and the inherently public nature of many civil society organizations and staff exposes them to heightened risks. Specifically, civil society organizations and individuals often have a significant online presence via corporate websites, social media advocacy, geopolitical publications, and press releases. State-sponsored actors use this information to:

- Scope and prioritize post-compromise objectives;
- Identify targets, including individuals for potential phishing campaigns; and
- Gather device and network information (such as IP addresses and operating systems).

Threat actors also use phishing, a form of social engineering, to steal login credentials for initial network access. In these instances, the threat actors pose as trustworthy sources (e.g., colleagues, acquaintances, or organizations) to lure victims into providing their login credentials—often by entering the credentials in a threat actor-controlled site to capture them.

State-sponsored actors invest substantial time and resources crafting identities for phishing attempts, leading to meticulously tailored attempts (this is specifically known as "spearphishing").

†† In the cybercommunity, malicious behaviors are commonly defined as tactics, techniques, and procedures (TTPs).

‡‡ For more information, see: attack.mitre.org and joint guide Best Practices for MITRE ATT&CK Mapping.

While predominantly executed via email, threat actors adapt their tactics to high-risk communities' communication preferences, leveraging text messaging, social media platforms, and diverse digital channels used for research and advocacy.

Example – Velvet Chollima: Velvet Chollima conducts reconnaissance to gather intelligence on the target's mission, interests, and professional contacts. As part of their reconnaissance, Velvet Chollima has tricked users into entering their credentials on a fraudulent webpage resembling the Google login page. They gained the victim's login details, allowing access for follow-on activities.

MITRE ATT&CK Mapping: See Table 1 for known reconnaissance techniques mapped to the MITRE ATT&CK for Enterprise framework.

Table 1: MITRE ATT&CK Reconnassiance Techniques

Technique Title	ID	Description
Gather Victim Org Information	T1591	Malicious actors gather information about the target organization (or target individuals' organization) that can be used for future operations.
Search Open Websites/Domains	T1593	Malicious actors search websites and/or domains for information about targets that can be used for future operations
Search Open Websites/Domains: Social Media	T1593.001	Malicious actors search social media for information about targets that can be used for future operations
Gather Victim Identity Information	T1589	Malicious actors gather information about the target individual or target organizations' staff that can be used for future operations. Information about identities may include a variety of details, including personal data (e.g., employee names, email addresses) as well as sensitive details such as credentials.
Gather Victim Host Information	T1592	Malicious actors gather information from victim hosts (devices, computers, servers) that can be used during targeting. Information about hosts may include a variety of details, including administrative data (e.g., assigned IP address) as well as specifics regarding its configuration (operating system).

Technique Title	ID	Description
Gather Victim Network Information	T1590	Malicious actors gather information about the victim's networks that can be used during targeting. Information about networks may include a variety of details, including administrative data (e.g., IP addresses, domain names) as well as specifics regarding its topology and operations.
Phishing for Information	T1598	Malicious actors send phishing messages to elicit sensitive information (e.g., login credentials) that can be used for future operations.

Tactic: Initial Access [TA0001]

Definition: Initial access is when malicious cyber actors attempt to gain access to a target network.

Description of Known Initial Access Techniques: Advanced persistent threat (APT) actors use credentials obtained via their phishing attempts (see the Reconnaissance section) to gain access to networks.

APT actors also leverage malware-based phishing to obtain initial access to targets. In malware-based phishing attacks, malicious actors pose as trustworthy sources to lure a victim into interacting with a malicious hyperlink or opening an email attachment to execute malware on host systems. The malware deployed enables data theft, surveillance, or advanced cyber intrusions. **Note:** Phishing is often made easier by the prevalence of well-known weaknesses in software that actors exploit to deliver their malware payloads.

Examples: APT groups associated with Iran, China, North Korea, and Russia integrate spearphishing emails into broader campaigns aimed at high-risk communities. These groups deploy tailored and, highly convincing messages to prompt users to engage with links or attachments.

Velvet Chollima: Velvet Chollima threat actors have been observed posing as a journalist seeking an interview or adopting the guise of an academic soliciting survey participation. Establishing trust through a sequence of initial emails, Velvet Chollima tactically introduces malicious elements in subsequent communications, usually via deceptive links or attachments. Notably, these links frequently conceal malware that provides Velvet Chollima with unauthorized access to the victim's personal computer and facilitating the surveillance of the victim's communications.

Additionally, Velvet Chollima has established auto-forward rules within a victim's email account, ensuring continuous monitoring of communications even if direct access to the account is lost.

Velvet Chollima's spearphishing operations showcase a nuanced and targeted cyber espionage strategy, employing social engineering and malicious payloads to infiltrate and monitor the communications of high-value targets.

Mustang Panda: The group's preferred initial intrusion vector is spearphishing emails, primarily to deploy remote access Trojans. This facilitates remote control of the target's computer, enabling comprehensive surveillance of the user's activities. Mustang Panda employs strategic tactics to entice targets into clicking on links or attachments, often referencing current events, and incorporating malicious versions of legitimate or stolen documents. For instance, in January 2022, emails sent to European targets included an attachment to a decoy European Commission report and a link to a European Union press release on human rights priorities.

Upon gaining initial access, Mustang Panda utilizes sophisticated techniques for prolonged and covert surveillance. In several instances, the group demonstrated its ability to monitor and exfiltrate data over extended periods, showcasing a capacity to remain undetected within an organization's network.

Charming Kitten: Using diverse online communication platforms, Charming Kitten executes advanced social engineering operations. The APT group strategically assumes personas, such as a journalist or NGO employee personas, engaging targets in deceptive conversations to establish trust before deploying malicious files or links. In May 2020, IBM X-Force uncovered 40 gigabytes of Charming Kitten's training videos, providing insights into their methodologies for data exfiltration from prominent email platforms.

MITRE ATT&CK for Enterprise Mapping: See Table 2 for initial access techniques mapped to the MITRE ATT&CK framework.

Table 2: MITRE ATT&CK for Enterprise: Initial Access Techniques

Technique Title	ID	Use
Phishing	T1566	Malicious actors send phishing messages to gain access to victim systems. The messages result in code execution or malware download on victim systems.
Phishing: Spearphishing Attachment	T1566.001	Malicious actors send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems.
Phishing: Spearphishing Link	T1566.002	Malicious actors send spearphishing emails with a malicious link in an attempt to gain access to victim systems. The links lead to the download of malware to the victim system generally via social engineering encouraging recipients to actively click or copy the URL (this requires the related technique User Execution [T1204]).

Mobile

Tactic: Initial Access [TA0027], Discovery [TA0032], Collection [TA0035], and Command Control [TA0037]

Definitions: Initial access is when malicious cyber actors attempt to gain access to a target mobile device. Discovery occurs when actors try and learn about the device in support of their operations. Collection is when actors try to gather data from a device. Command and control is when actors try to communicate with compromised devices to control them.

Description of Known Techniques: Actors use phishing to gain access to devices, often through SMS. They also use Trojanized apps. Users download these seemingly legitimate apps that house malicious software enabling actors to access of sensitive user information, including call logs and geolocation data, and to take over a user's device.

After gaining access to devices, actors often install spyware, such as Pegasus and Intellexa, on the devices. Spyware is a tool that provides extensive surveillance capabilities, including location tracking, image and audio capture, and access to personal files and communications.

Examples: The examples below identify how state-sponsored actors use Trojanized applications and Spyware in their campaigns.

Earth Empusa: In 2021, Meta reported that Earth Empusa established deceptive websites resembling third-party Android app stores. These decoy platforms hosted applications tailored for a Uyghur (Turkic ethnic group originating from and culturally affiliated with the generalized regions of Central and Eastern China) audience, including a keyboard app, prayer app, and dictionary app.

Analysis by TrendMicro revealed that upon downloading these apps, the user's device became infected with malware. The malicious software orchestrated by Earth Empusa aimed to collect a range of sensitive data, including geolocation information, call logs, and SMS messages. Additionally, the malware granted unauthorized access to the device's camera, microphone, and screenshot capabilities, exemplifying the group's advanced and intrusive surveillance techniques.

APT-C-27; To compromise the security of these individuals, APT-C-27 ingeniously crafted malicious applications, among them an app named VPN Secure, alongside decoy versions of popular communication platforms such as Telegram and a Syrian news application. This strategic use of seemingly innocuous applications reflects a sophisticated approach by APT-C-27 in its pursuit of undermining the security and privacy of its targeted subjects.

APT-C-27 conducted a second campaign targeting Free Syrian Army affiliates and former military personnel. Leveraging social engineering, the group tricked individuals into clicking on links leading to deceptive websites mimicking popular services like Telegram and Facebook.

MITRE ATT&CK for Mobile Mapping: See Table 3–Table 6 for techniques mapped to the MITRE ATT&CK for Mobile framework.

Table 3: MITRE ATT&CK for Mobile: Initial Access Techniques

Technique Title	ID	Description
Phishing	T1660	Malicious actors send malicious content to gain access to victim devices.

Table 4: MITRE ATT&CK for Mobile: Discovery Techniques

Technique Title	ID	Description
Location Tracking	T1430	Malicious actors track a device's physical location.

Table 5: MITRE ATT&CK for Mobile: Collection Techniques

Technique Title	ID	Description
Protected User Data: Call Log	T1636.002	Malicious actors gather call log data.
Protected User Data: SMS Messages	T1636.004	Malicious actors gather SMS messages.
Video Capture	T1512	Malicious actors use a device's cameras to gather information by capturing video recordings. Malicious actors may also capture images at specified intervals in lieu of video files.
Audio Capture	T1429	Malicious actors capture audio, for example user conversations, surroundings, and phone calls.
Screen Capture	T1513	Malicious actors use screen capture to collect information about a target device, such as applications running in the foreground, user data, and credentials.

Table 6: MITRE ATT&CK for Mobile: Command and Control Techniques

Technique Title	ID	Use
Ingress Tool Transfer	T1544	Malicious actors transfer tools, files, or malware to a victim device from an external system.

References

[1] See "Microsoft Digital Defense Report 2023," October 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023. Microsoft's *Digital Defense Report 2023* reports APT threat activity against think tanks, NGOs, media, and human rights activists emerging from Russia (Nobelium, Strontium, Seaborgium), China (Nickel, Gadolinium), North Korea (Osmium), and Iran (Phosphorus).
[2] See "CrowdStrike Threat Landscape: APTs & Adversary Groups," CrowdStrike, n.d, https://www.crowdstrike.com/adversaries/. According to CrowdStrike's Global Threat Landscape, from August 18 to November 16, 2023, APTs from Iran (Charming Kitten), China (Phantom Panda, Aquatic Panda), and North Korea (Velvet Chollima, Ricochet Chollima) represented potential threats to think tanks.
[3] See "CrowdStrike Threat Landscape: APTs & Adversary Groups," CrowdStrike, n.d, https://www.crowdstrike.com/adversaries/. According to CrowdStrike's Global Threat Landscape, from August 18 to November 16, 2023, APTs from Iran (Static Kitten, Haywire Kitten, Charming Kitten), China (Cascade Panda, Overcast Panda, Aquatic Panda, Emissary Panda), the Russian Federation (Fancy Bear, Gossamer Bear), and North Korea (Velvet Chollima, Ricochet Chollima) represented potential threats to NGOs.
[4] See "CrowdStrike Threat Landscape: APTs & Adversary Groups," CrowdStrike, n.d, https://www.crowdstrike.com/adversaries/. According to CrowdStrike's Global Threat Landscape, from August 18 to November 16, 2023, a North Korean APT (Ricochet Chollima) and Iranian APT (Charming Kitten) represented potential threats to dissidents.
[5] See "CrowdStrike Threat Landscape: APTs & Adversary Groups," CrowdStrike, n.d, https://www.crowdstrike.com/adversaries/. According to CrowdStrike's Global Threat Landscape, from August 18 to November 16, 2023, a Russian APT (Fancy Bear) represented a potential threat to nonprofits.
[6] See "Project Galileo 9th Anniversary" (Cloudflare Radar, June 5, 2023), https://radar.cloudflare.com/reports/project-galileo-9th-anniv.
[7] See Cloudflare Radar, "DDoS Attack Trends for 2023 Q2" (Cloudflare Radar, July 18, 2023), https://radar.cloudflare.com/reports/ddos-2023-q2.
[8] See Cloudflare Radar, "DDoS Attack Trends for 2023 Q3" (Cloudflare Radar, October 26, 2023), https://radar.cloudflare.com/reports/ddos-2023-q3.
[9] See "ENISA Threat Landscape 2023," ENISA, October 19, 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.
[10] See CrowdStrike, "Velvet Chollima" crowdstrike.com, February 25, 2023, https://www.crowdstrike.com/adversaries/velvet-chollima/.
[11] See "BRONZE PRESIDENT Targets NGOs," Secureworks, n.d., https://www.secureworks.com/research/bronze-president-targets-ngos.
[12] See Certfa Lab, "Charming Kitten: 'Can We Have a Meeting?'" Certfa, n.d., https://blog.certfa.com/posts/charming-kitten-can-we-wave-a-meeting/.
[13] See "ITG18: Operational Security Errors Continue to Plague Sizable Iranian Threat Group," Security Intelligence, August 23, 2023, https://securityintelligence.com/posts/itg18-operational-security-errors-plague-iranian-threat-group/.
[14] See Mike Dvilyanski and Nathaniel Gleicher, "Taking Action Against Hackers in China," *Meta*, April 20, 2021, https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china/.
[15] See CitizenLab "Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits" September 24, 2019, https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/.
[16] See Volexity Blog "Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs" September 2, 2019, https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/.
[17] See Mike Dvilyanski and David Agranovich, "Taking Action Against Hackers in Pakistan and Syria," *Meta*, November 16, 2021, https://about.fb.com/news/2021/11/taking-action-against-hackers-in-pakistan-and-syria/amp/.