
Kdo Cy · Cdmt Cy · Cdo Ci

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Schweizer Armee
Kommando Cyber

Insights in recent threats and state attacks

21.03.2024, Zurich

Juan Ramos,
Head of Cyber Threat Research and Analysis team
CNO – Computer Network Operations
CEA - Cyber und Elektromagnetische Aktionen
Kommando Cyber federal office

Threat Actors Activities for 2023

- Global overview
- View on the Israel - Palestine conflict
- Summary of 2023 – beginning of 2024

China

China Q1

General:

- Sustained activity of high intensity and global reach.
- Targets sectors: government, technology and telecommunications.
- Tools and Malware:
  - Cobalt Strike and SoftEther VPN public tools.
  - ShadowPad development and customization.
  - New malware families: MQTTRat.

Aquatic Panda (Earth Lusca):

- Maintains high activity and adopts Brute Ratel C4 tool and exploits vulnerability in Fastjson Java Library.

China Q2

Intrusions:

- Maintain high activity, focusing on East Asia and Southeast Asia.
- Emphasis on health, technology and telecommunications sectors.
- Four new malware families: RATs and mail dumping tools.

Volt Typhoon:

- Identified in multiple US targets.
- Exploitation of vulnerabilities, persistence through webshells, and living-off-the-land techniques.

ChamelGang:

- Intense activity in health and technology, with the use of novel techniques.
- Deployment of new Linux RAT (LegalSmash, detected by crowdstrike) and infrastructure obfuscation techniques.

Gallium:

- Expansion into non-traditional sectors, such as non-profit.
- Updated tools and geographic expansion indicate adaptation and continuous improvement of techniques.

China Q3/Q4

General Activity:

- Maintain high levels of activity.
- Main focus on telecommunications, government and technology entities in East and Southeast Asia.

Tools Discovered:

- Four new malware families identified: ValleyRat, FlashKey, StealthyUSB and PingPull.
- Intrusion operations targeting a government in Southeast Asia.

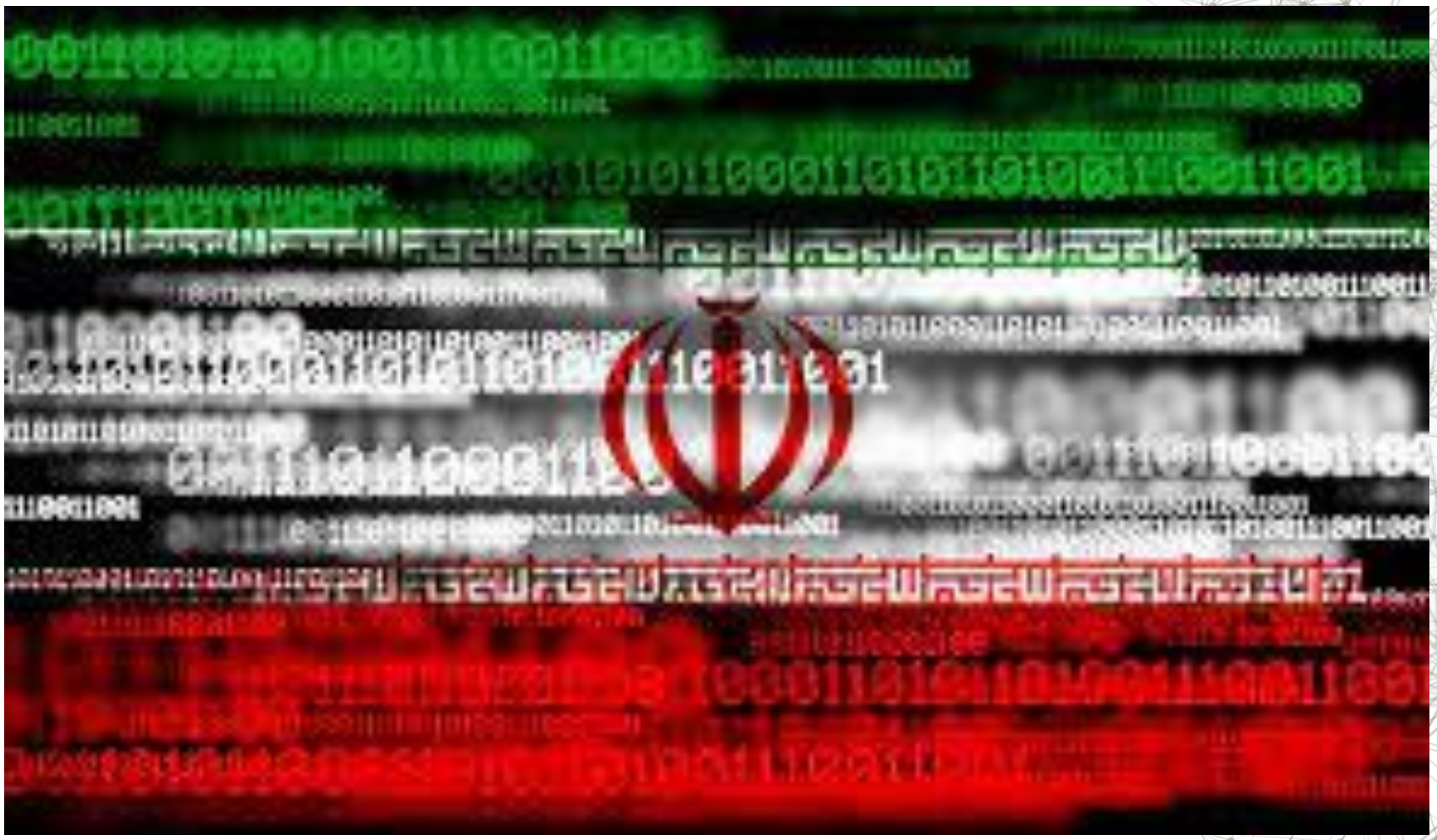
Operations Highlights – Gallium:

- Incident of an NGO in the U.S.
- Exploitation of a vulnerability in the IIS server.
- Use of tools such as Rclone and an ASPX webshell.
- Subsequent activity in September with a PingBok executable on the same entity.

Featured Operations - Flax Typhoon:

- Related activity since November 2022.
- Identification of a Keyplug backdoor configured with a C2 address in September 2023.
- Use of the Keyplug malware, being the second Chinese adversary to use it after APT41.

Iran



Iran Q1

Opportunistic Exploitation:

- APT35 (Charming Kitten) exploits opportunities for initial access in several sectors.

Telecommunications Intrusions:

- Tracer Kitten attacks a telecommunications provider in South Asia.
- DNSDAT malware updates and new tools identified.

Continuous Remote Exploitation:

- ManageEngine vulnerability in legal entity in Europe.
- IBM Aspera Faspex vulnerability in North American technology organization.
- Possible exploitation of SysAid application in municipal government in North America by MuddyWater.

Iran Q2

Permanent Objective: Targeting primarily organizations in the Middle East and North Africa (MENA) region, with a focus on government, telecommunications and academic sectors.

APT39 (Helix Kitten) and Cobalt Lyceum use new tools and target energy and telecommunication sectors.

APT35 (Charming Kitten) continues to refine its operations, using targeted phishing attacks and staged infection mechanisms to make analysis more difficult.

- Spear-phishing operations targeting policy researchers in MENA, deploys PowerWindow malware.
- APT35 reacts quickly to real political events, such as elections, to gather valuable intelligence.

Iran Q3/Q4

Geographic Focus:

- Adversaries centered primarily in (MENA), affecting energy, government and technology sectors.

Haywire Kitten Influence operations:

- Linked to Iranian contractor Emenet Pasargad, conducted cyber influence operations using new identities and data leaks.
- Infrastructure used to express hostile rhetoric and disseminate personal information of Israeli citizens in criminal forums.

Russia

Russia Q1

Russian Intelligence Operations:

- Extensive intelligence gathering activities
- Spear-phishing by Gamaredon Group and APT29 (Cozy Bear) in Ukraine and Eastern Europe.
- Limited destructive activity, reflecting Russian military uncertainty.

UAC-0056 (SaintBear):

- Website defacement on the anniversary of the Russian invasion of Ukraine.
- Continued data leak activity.
- Absence of attribution misdirection attempts.

APT28 (Fancy Bear):

- Continued use of credential harvesting tactics.
- Exploitation of zero-day vulnerability in Microsoft Outlook (CVE-2023-23397).
- Phishing campaigns focused on Ukrainian users.

Russia Q2

APT28 (Fancy Bear):

- Tactical Evolution: adapts and improves credential phishing operations, abandoning low-cost operations to focus on more sophisticated techniques.
- Mail Infrastructure Attacks: Switching to HTML attachments in emails that simulate web login pages, improving the BitB (Browser in the Browser) technique to limit detection.
- Vulnerability Exploits: continued exploiting vulnerabilities in email servers, abandoning exploit CVE-2023-23397 (Outlook vulnerabilities).
- Use of Compromised Edge Devices: Increasing reliance on compromised Edge SOHO device infrastructure for credential harvesting operations.

Destructive attacks in Ukraine:

- Continuity of destructive attacks: against Ukrainian organizations.
- Diversification of Tools: adoption of generic wiping methodologies using legitimate software to evade detection.
- Consistent approach: continued use of threat deployment from compromised Domain Controllers through Group Policy Objects (GPOs).
- Recent examples: deployment of RoarBat malware by BlackEnergy Group and custom deletion tool called Eraser.

Russia Q3/Q4

Geographic Focus and Target Sectors:

- Continued development of intelligence gathering capabilities, especially in Ukraine and allied nations.
- Primary target government and military sectors.

APT28 (Fancy Bear): Renewal of Access Efforts:

- Renewed efforts to gain access, combining vulnerability exploitation and spear-phishing campaigns.
- Resumption of attempts to exploit CVE-2023-23397 (Outlook) at the end of August 2023.
- Exploitation of vulnerability in WinRAR and large-scale spear phishing against government and military organizations.

BlackEnergy Mobile Malware Deployment on Android Devices:

- Campaign disclosed by Ukrainian Security Services against Android devices used by Ukrainian military personnel.
- Deployment of custom and open source intelligence gathering tools, including identification and data collection from Starlink systems used by Ukrainian armed forces.

Summary of 2023 – beginning of 2024

- **Same trend for this beginning of the year with similar objectives.**

- **Know your adversary**
  - We don’t have malware problem. We have an adversary problem.

- **Integrated Intelligence**
  - Threat intelligence is the DNA that should drive all aspects of public and private organizations to protect themselves.

- **Protect what matters**
  - To stop an adversary, we must first understand their tactics, techniques and motivations.
  - We must adapt quickly.


Any
Question