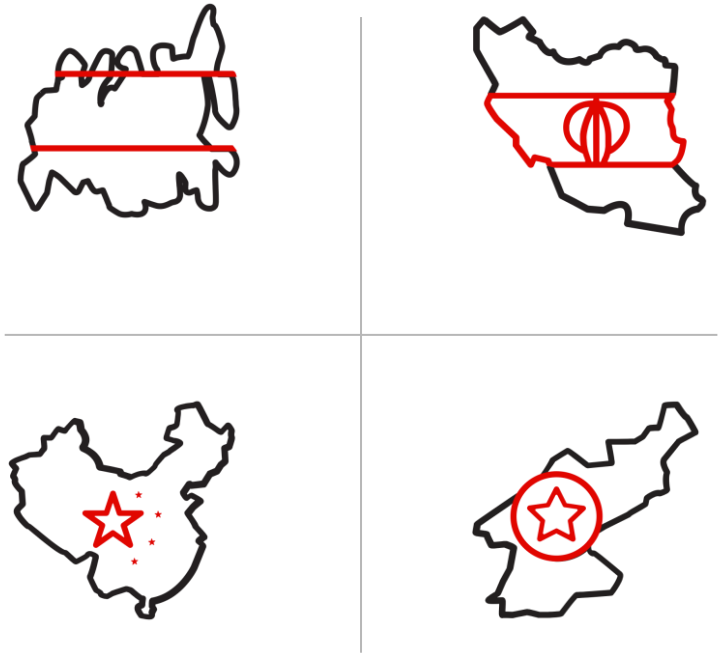
The Evolving Cyber Threat Landscape

30 January 2025 | Blake Djavaherian

Google Cloud Security

State-Nexus Threats

The Big Four



The Big Four

Russia

- Continued espionage and IO focus on the Ukraine conflict; secondary emphasis on various entities across NATO countries.
- Use of direct targeting or downstream compromise to access intended targets.

China

- Ongoing development of novel malware ecosystems for embedded systems.
- Continued deployment of new obfuscation networks and zero-day exploits.

Iran

- Ongoing tensions within the Middle East and North Africa (MENA) region and with the West fueling operations.
- Primary targeting of government and telecommunications organizations across MENA.

North Korea

- Espionage targeting government, defense, education, think tank targets primarily in South Korea and the U.S.
- Revenue generation to support regime interests through IT workers (ITW), cryptocurrency theft, and extortion tactics.

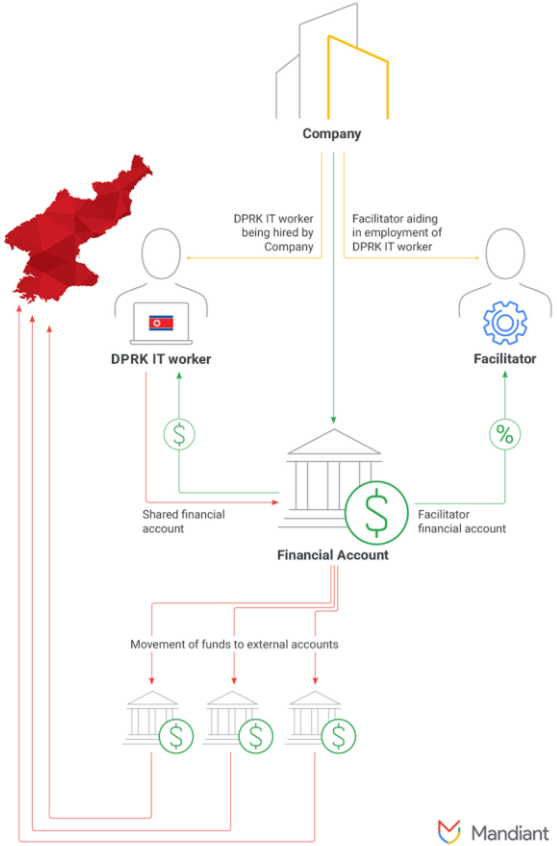
The Two Sides of DPRK Cyber

Revenue Generation:

- The DPRK continues to deploy vast numbers of individuals to farm Western employment opportunities for state revenue.
- Due to increasing scrutiny, two updates:
  - Greater likelihood of retaliatory extortion following termination.
  - ITWs have started altering infrastructure following detection, such as changing VOIP numbers.
- Additionally, the DPRK conducts compromises for cryptocurrency theft, reflecting crypto's intrinsic laundering-enablement properties.

Cyber Espionage:

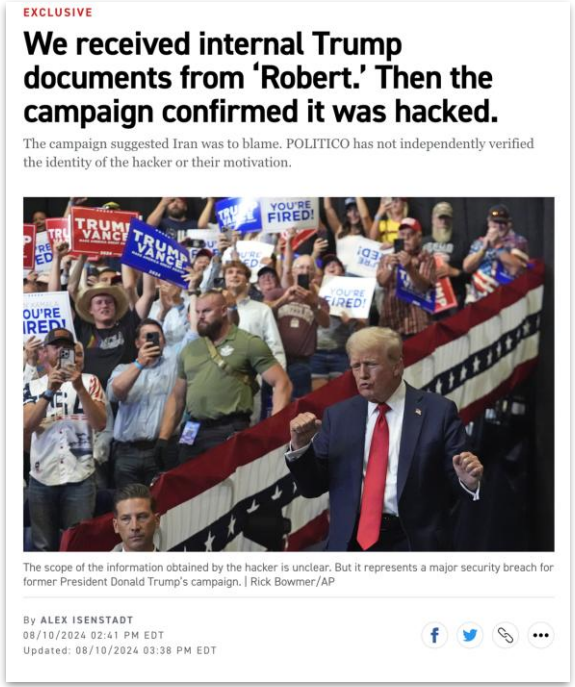
- Continued intelligence collection operations using various capabilities, including supply chain compromise.



Iranian Hybrid Operation Enablement

August 2024 Trump Campaign Compromise:

- Information allegedly stolen included internal documents discussing the Trump campaign's VP-decision making process.
- The actor attempted to distribute the information by sending digital copies anonymously to at least one reputable news agency.
- Activity attributed to APT42 based on infrastructure and TTP overlaps.



EXCLUSIVE

We received internal Trump documents from 'Robert.' Then the campaign confirmed it was hacked.

The campaign suggested Iran was to blame. POLITICO has not independently verified the identity of the hacker or their motivation.

The scope of the information obtained by the hacker is unclear. But it represents a major security breach for former President Donald Trump's campaign. | Rick Bowmer/AP

By ALEX ISENSTADT
08/10/2024 02:41 PM EDT
Updated: 08/10/2024 03:38 PM EDT

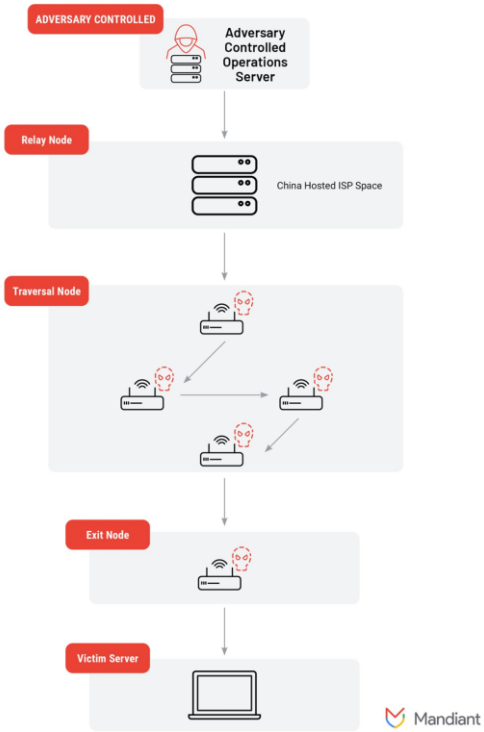
Chinese Technical Development & Positioning

Ongoing, Institutionalized Capability Expansion:

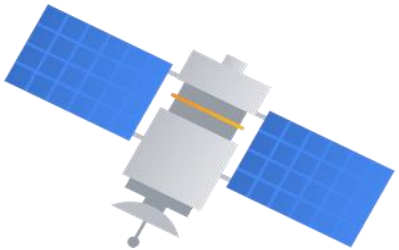
- Regularized creation and deployment of novel zero-day capabilities to facilitate access and evade any potential existing detections.
- Refurbishment, creation, and iteration of malware ecosystems to fit diverse operational requirements.

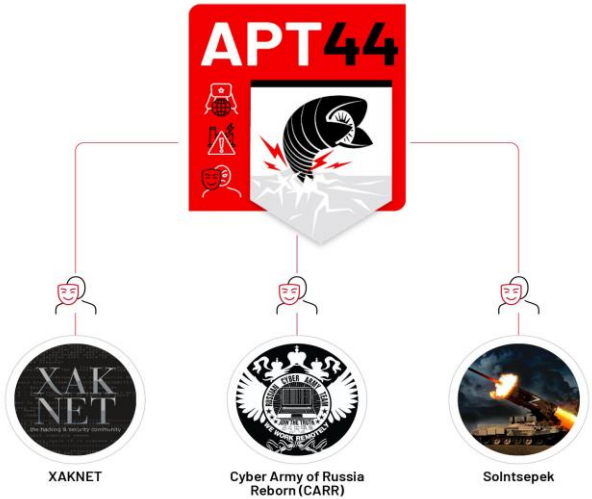
Operational Obfuscation at Scale:

- Frequent reliance on sophisticated living-off-the-land (LOTL) tactics to reduce operational footprint and likelihood of detection.
- Development and operational use of custom anonymization networks to mask the origin and consistency of malicious infrastructure.
- Targeting of edge devices to enable initial access as well as re-access to networks belonging to organizations of interest.



Russian Focus on Ukraine





Criminal Threats

Continued Potential for Criminal Spillover

ROYAL Ransomware Disables Dallas City Functions:

- On 06 Sept. 2023, the City of Dallas released an AAR detailing a mid-2023 ransomware event against city systems.
- The City's report provided additional insight into adversary dwell time, specific service disruptions, and the direct costs of the incident (~$8.5 million).

RANSOMEDVC Targets D.C. Board of Elections:

- On 06 Oct. 2023, the Washington, D.C., Board of Elections (DCBOE) announced their awareness that on 05 Oct. the group RANSOMEDVC claimed access to voter data.
- According to DCBOE, their investigation showed that the information was stolen through a breach of an externally hosted web server.

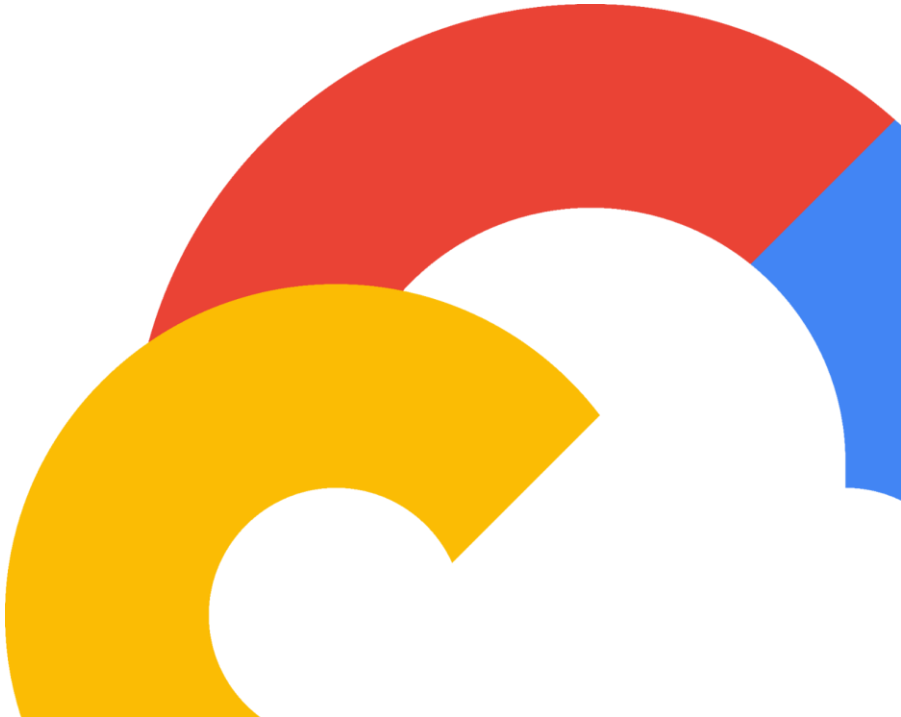
Evolutions in the Ransomware Ecosystem

Ascendence of Newer RaaS Groups:

- Law enforcement crackdowns leading to the reformation of ransomware group structures
  - For example, the leading RaaS by volume, RANSOMHUB, emerged February 2024 and has since capitalized on newfound instability.

- Resultant ecosystem rewards flexibility, OPSEC, and individual dissociation from any single ransomware enterprise.

Thank you



Google Cloud