Cyber-Intelligence Report

This cyber-intelligence product is a snapshot of selected cyber events. Collection of information is in accordance with clients' guidelines. It contains 'observations', meaning headlines and links to online information. It *MAY* contain comments and analysis. It is copyright David Swan 2026. This report is **TLP:CLEAR**[1] and MAY be shared freely.

If this report does not meet your requirements, is in error or if you need additional information, contact David Swan at DSC.Ops.Vulcan@gmail.com

Cyber Intelligence Report: Israeli Hacking Campaigns

This report contains selected cyber-security information from 12th to 25th June 2026.

Synopsis

1. Israel currently has three interesting cyber campaigns of note: the Popa BotNet lives in Android TV boxes and a variety of streaming services, Israel is suspected of hacking four Iranian banks, and an Israeli organization has been identified running information operations in multiple countries. The PRC continues to quietly siphon up intellectual property. 'i-Soon', a PRC company, has expanded its hacking tools to include 'Windows'. The 'FortiNet' hack is a Russian credential theft campaign. A Russian software company was DDoSed, and NoName057(16) attacked Belgian websites. Law enforcement uses a new tool against hackers.

2. We report hacker activity based on the threat posed. It is our *assessment* that cyber conflicts such as Russia vs Ukraine, Iran vs Israel, etc are the most likely sources for the creation of next generation malware and/or a primary source of cyber attacks.

Israeli Cyber Campaigns

3. **'Popa' Botnet Linked to Publicly-Traded Israeli Firm**. Researchers from multiple security firms have concluded that an Israeli firm 'Alarum Technologies Ltd', is behind the operation of a sprawling Android-based botnet called Popa. Popa "*Implements a persistent communications layer capable of registering a device, maintaining long-lived encrypted connections, and opening communication tunnels on demand. ... the security firm Qurium described how it stumbled on some of those same domains while investigating a series of disruptive and expensive data scraping events targeting the company's hosted organizations in May 2026, in which the scraping activity was scattered evenly across more than 1.4 million Internet addresses.*" The addresses were associated with Android-based TV boxes, "*marketed under thousands of brand names and model numbers and broadly available for purchase.*" One of the controlling domains is 'ninjatech[.]io' which in turn is associated with 'Ninjatech', a company founded by Moishi Kramer. According to his LinkedIn profile, Kramer "*says he is vice president of research and development at NetNut ... before the company was acquired by Alarum Technologies.*"[2] At least one source lists

1 Definition **TLP:CLEAR.** From U.S. Govt Cyber Defense Agency. Traffic Light Protocol (TLP) Definitions and Usage, Recipients may share this information without restriction. Information is subject to standard copyright rules.

2 Source: Krebs On Security. 'Popa' Botnet Linked to Publicly-Traded Israeli Firm

© David Swan Consulting 2026

Kramer as the owner of the Ninjatech domain.

4. Kramer denies any current knowledge or linkage to Popa, having sold his interest years ago. "*the proxy-tracking company Synthient said a recent analysis of the Popa SDK revealed outbound traffic clearly associated with NetNut. 'The research team assesses with high confidence that devices running Popa forward traffic from Netnut clients,' Synthient wrote. 'This proves without a shadow of a doubt that Popa actively continues to be used by NetNut as part of their proxy pool.' ... Qurium said it found several dozen domains used to control Popa that were all hosted in lockstep across multiple Internet addresses over time ...* [including] *in dozens of pirated or modded video content streaming apps, such as CRICFy, DooFlix, Sprozfy, RTS Tv, Flixoid, CyberFlix, Rapid Streamz, TvMob and HD/OceanStreams*"[3] in addition to dozens of Android TV boxes.

5. **Did Israel Hack Four Iranian Banks**? Following the U.S. granting Iran access to to billions in frozen funds, four Iranian banks were hacked in a cyber attack suspected to have been launched by Israel.[4] "*Disruptions in the online systems of ... Bank Melli, Bank Tejarat, Bank Saderat, and the Export Development Bank of Iran, have entered their tenth day.*" Remotes services have been severely affected, including "*conducting financial transactions and using online and mobile banking services. ... the source of the disruption was an attack on the shared core infrastructure and service layer of these banks. ... and supports parts of the country's payment networks, including Shetab and Shaparak. ... The exact origin of this attack has not yet been determined.*"[5]

6. News releases on 23 June say that Iran's banking has been 'frozen' due to a targeted cyber attack on 'related resources'.[6] No estimates for return to normal services were provided. Iranian refugees reported being unable to access any of their funds saying their money has 'disappeared'.[7]

7. **Israeli Firm 'BlackCore' Accused Of 'Meddling' in Elections**. Accusations are increasing against Israeli firm 'BlackCore' for mounting disinformation campaigns to affect elections in multiple countries. On 20 May Reuters published an report on French Interior Minister Laurent Nunez probing "*an alleged foreign interference campaign ... targeting at least three mayoral candidates from the France Unbowed (LFI) party.*" "*Reuters could not independently establish who was behind BlackCore, verify where it was based, or find any reference to the company in Israeli corporate records.*"[8] France's disinformation detection service, Viginum, says BlackCore is also suspected of "*meddling in elections in New York City and Scotland, and operating in Angola and Togo.*" Multiple law enforcement agencies in several countries either refused comment or did not reply to inquiries. "*Before scrubbing its online presence*

3 Source: Krebs On Security. 'Popa' Botnet Linked to Publicly-Traded Israeli Firm
4 Source: The Telegram (UK). Israel suspected of cyber attack on Iranian banks
5 Source: iranwire. Disruption at Four Major Iranian Banks Remains Unresolved
6 Source: Tabnak (Iran News Service). Announcement of the country's cyber command about banking disruption
7 Source: NewsNation. Iranians' money 'disappeared,' cannot be accessed in regime-controlled banks
8 Source: Reuters. French prosecutors probing alleged foreign interference against hard-left candidates, minister says

© David Swan Consulting 2026

following enquiries from Reuters, BlackCore described itself as 'an elite influence, cyber, and technology company built for the modern era of information warfare.' It said it provided governments and political campaigns with 'cutting-edge strategies, advanced tools, and robust security to shape narratives.' "[9]

People's Republic of China (PRC)

8. **PRC Continues to Siphon Intellectual Property.** A PRC cyber espionage crew being tracked by Google as UNC6508 has "*remained hidden in the networks of multiple North American medical and military research organizations for more than a year, deploying custom malware and snooping through Gmail inboxes and stealing sensitive data.*" Google's researchers noted: "*It's one of the most interesting grocery shopping lists of things to collect that I've seen from a state-sponsored actor.*" The range of topics included "*such esoteric topics as drone technology and a viral disease that spreads from mosquitoes to humans. ... The operation targeted several national, state, and private medical entities. These organizations comprise world-renowned clinical providers, premier academic centers, North American military health institutions, professional advocacy groups, and health regulatory bodies. ... Their research areas span a broad spectrum of modern medicine, from molecular discovery and clinical drug trials to state-level public health policy and military readiness.*"[10]

9. **PRC Contractor 'i-Soon' Now Hacking 'Windows**. ESET researchers have discovered two undocumented Windows variants of SprySOCKS, a 'backdoor' program that used to be unique to Linux. While ESET tracks the attackers as 'FishMonger', they're also known as 'Aquatic Panda', 'Charcoal Typhoon', and 'RedHotel'. This cyber team is operated by the PRC firm 'i-Soon'. The report did not say who was being targeted, only that the new variants of SprySocks would increase i-Soon's espionage scope.[11]

Russia

10. **Hack Of Fortinet Firewall Is Russian Credential Theft Campaign**. A hacking campaign named 'FortiBleed' has been targeting FortiNet Firewalls. "*FortiBleed is a large-scale, financially motivated campaign targeting FortiGate firewalls globally. ... The numbers alone are staggering: over 430,000 FortiGate firewalls targeted, more than 110 million credentials identified across 659+ harvesting pipelines, and a confirmed breach of a NATO-aligned defense contractor. ... the campaign is still actively sniffing over 19,000 devices, part of a broader pool of 80,553 identified targets. ... The victim profile skews heavily toward SMBs: roughly 66% of affected organizations have fewer than 200 employees, and nearly 90% have annual revenues below $100 million.*"[12] "*Attackers compromise exposed firewalls, harvest the authentication traffic and credentials passing through them, crack what they capture,*

9 Source: Reuters. Israeli firm BlackCore suspected of meddling in New York and Scotland votes, France says
10 Source: The Register. PRC-linked spies hid inside medical and military networks for more than a year, snooping through Gmail and stealing data
11 Source: Security Affairs. China-Linked FishMonger Ports SprySOCKS to Windows With Kernel-Level Stealth and UEFI Bootkit Hints
12 Source: Security Affairs. FortiBleed: The Most Detailed Breakdown Yet of an Active Russian Credential-Harvesting Operation

© David Swan Consulting 2026

and sell that access, ... The defense contractor's compromise suggests the threat actor behind FortiBleed, likely a Russian-speaking APT, may collaborate with Russian state-sponsored groups. However, it may also sell acquired access to ransomware gangs."[13]

11. **Russian Software Company 'cyberattacked'.** Kaluga Astral, a Russian software company, was hit by a cyber attack that disrupted its services for a week. "*Kaluga Astral develops electronic document management software, digital reporting systems for government agencies and cybersecurity products. Founded in 1993, the company reportedly serves government institutions, banks and large state-owned enterprises, including Russian Post and Moscow public transport operator Mosgortrans. ... According to customer complaints, the disruption affected a range of services used by businesses, leading to interruptions in cash register operations, difficulties selling certain regulated goods, loss of access to customer portals and corporate email and problems with electronic human resources document management systems and authentication using digital certificates.*"[14]

12. **NoName057(16) Targeted Belgian Websites.** Following the meeting of NATO Defense Ministers in Brussels on 18 June, Russian hacking group NoName057(16) hit Belgian website with DDoS attacks. Targeted websites included: "*the Walloon Parliament and the federal science policy agency BELSPO.*" Belgian sources report 'only limited disruption.'[15]

Organized Crime Legislation Used to Prosecute Hackers

13. Multiple security companies and law enforcement agencies collaborated to take down "*more than 200 domains and command-and-control (C2) servers that formed the backbone of StealC and Amadey infrastructure.*" What makes 'Operation Endgame' unique is the first use of AI (Artificial Intelligence) and organized crime legislation (Racketeer Influenced and Corrupt Organizations Act (RICO)). "*a Europol-led law enforcement coalition flagged and restricted cryptocurrency assets valued at more than $47 million and recovered about 27 million stolen credentials.*"[16] It is not clear how the use of organized crime legislation changed the investigation.

This cyber-intelligence product is produced by David Swan. It is copyright David Swan 2026. This report is **TLP:CLEAR**[17] and MAY be shared freely.

To unsubscribe from this service send an email to DSC.Ops.Vulcan@gmail.com

13 Source: Security Week. Russian Initial Access Broker Behind FortiBleed Campaign
14 Source: The Record. Cyberattack on Russian tech firm Astral disrupts business, government services for week
15 Source: Belgian News Agency. Pro-Russian hackers target Belgian websites after NATO ministers' meeting
16 Source: The Register. Microsoft uses AI to link two malware operations in racketeering suit
17 Definition **TLP: CLEAR.** From U.S. Govt Cyber Defense Agency. Traffic Light Protocol (TLP) Definitions and Usage, Recipients may share this information without restriction. Information is subject to standard copyright rules.

© David Swan Consulting 2026