



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: Russia, PRC and Iran

This report contains selected cyber-security information from 18th September to 1st October 2026.

Synopsis

1. Russia's '[Star Blizzard](#)' hackers launch campaign with new malware. [Russia's 'patriotic hackers' targeting EU's operational technology](#) (OT). Hackers attacking Russia hit fast food chains '[Burger King](#)' and '[Dodo Pizza](#)'. A PRC hacker leverages AI to [hit retailers and credit cards](#). [Salt Typhoon now targeting South America](#). Iran's hackers are busy. '[Chosen Brick](#)' campaign targets regime opponents, while a number of [other campaigns try for destructive impact](#).
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.

Russia's Cyberwar

3. **Russia's 'Star Blizzard' Launches New Campaign.** One of the Russian Federal Security Service (FSB) Centre 18's hacking teams, 'Star Blizzard', "*has been relying on large-scale phishing attacks and a new malware delivery technique dubbed RedFlick, which requires a single user interaction for malware execution.*" If the target clicks on the lure, "*a PDF document that, opens a decoy file while quietly executing a background script. That script fetches an MSI installer, configures scheduled tasks for persistence, and launches the NoroBot or BaitSwitch downloader to deliver the CosmicPulse Python backdoor. ... Star Blizzard, Microsoft says, has been creating accounts on compromised websites to send tens to hundreds of phishing emails per campaign, likely through a mass-mailing phishing platform. ... [they are using] the technique in attacks against Ukrainian individuals and institutions, as well as international NGOs, think tanks, governments, and financial institutions that have been providing support to Ukraine.*"²

4. **Russia's Hackers Conducting Attacks on 'OT'.** The European Union Agency for Cybersecurity is warning that pro-Russia hacktivist groups, including NoName057(16),

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: Security Week. [Russian APT Star Blizzard Uses 'RedFlick' Infection Chain in Recent Attacks](#)



Cyber-Intelligence Report

are increasingly attacking operational technology and industrial environments. *"hacktivist DDoS attacks generally caused little disruption ... [but now] there is reason for concern ... Operational technology systems are particularly deployed within organizations involved in critical sectors, such as the energy sector, telecommunications and transport. ... According to ENISA, the most prolific hacktivist group involved in these attacks was the pro-Russia NoName057(16). ... ENISA observed continued integration of AI into malicious activities last year - by both criminals and state-linked actors - and expects its next report to show that trend continuing this year. AI will act as a "force multiplier" across all types of threats, Boutemour said, from crafting more believable phishing messages to creating proof-of-concept vulnerability exploits."*³

5. Hacker Breaches Russia's 'Burger King'. *"Russian Burger King patrons have been left with a bad taste after cyber crooks flame-broiled 3.2 million customers in a whopper of a breach, serving up their personal data for anyone hungry enough to consume it. ... The attackers flipped names, dates of birth, email addresses, and phone numbers, with a side order of genders and approximate geographic locations. ... The information stolen in the breach was well-seasoned: it spanned more than six years, dating back to May 2018."*⁴

6. Russia's 'Dodo Pizza' Confirms Cyberattack. *"The hacker group DATASUCKERS claims to have stolen 2-3 TB of data. ... Dodo.Brands operates over 1,300 pizzerias and coffee shops across 26 countries, including Russia and Kazakhstan." This translates to "approximately 68 million customers across all countries where the network operates, including Kazakhstan. ... exposed data may include: Full names, Physical addresses, Email addresses and phone numbers, Dates of birth, [and] Order history."*⁵

7. Assessment: Despite reorganization, retooling of malware, and the introduction of AI to Russia's hackers, Russia has been unable to defeat or even 'slow down' Ukraine's Internet environment. Russia has been on the receiving end of pointed attacks on its government, defence supply chain, and now increasingly on highly visible public services. The inability of some Russians to order their pizza online will drive home the effects of the war with Ukraine in a personal way that is very difficult to counter. Russia has been more successful with its cyber espionage and cyber sabotage efforts against Europe. Those campaigns are ongoing.

People's Republic of China

8. Enterprising PRC Hacker Leverages AI And Targets Retailers. AI security company Gambit identified a human driven AI campaign that hit at least "105 attacks, and compromised, 'to varying degrees,' at least 27 companies" between 10 to 15 September. The hacker used "three different open source AI harnesses - Strix, Cairn, and Hermes - to run the near-autonomous attacks and hit "tens" of companies each day."

3 Source: Govinfosecurity. [Pro-Russia Hacktivists Increase OT Intrusion Claims Across EU](#)

4 Source: The Register. [Well-done hack flames 3.2M Burger King Russia users](#)

5 Source: Pravda.ru. [Russian pizza restaurant chain confirms cyberattack: Hackers claim 68 million users exposed](#)



Cyber-Intelligence Report

- *"Hermes acted as the campaign orchestrator. The always-on AI assistant acts independently to execute multi-step tasks and manage workflows, and it can write and edit its own skills."*
- *"Strix, an open source penetration testing tool, [was used] to search for vulnerabilities to exploit at targeted organizations."*
- *"Cairn, another autonomous penetration testing AI tool ... receives target domains and an attack objective - like deploy a shell, or achieve admin access. It then runs until it either achieves the objective, times out, or is stopped by a human. Between September 10 and 15, Cairn launched 105 attack projects."*⁶

9. 'Salt Typhoon' Targets South America. Cyber security company ESET is warning that PRC government hackers 'Salt Typhoon' have developed a new 'backdoor' and *"shifted its focus to Latin America ... from mid-2025 into 2026, the vast majority - 90 percent - of Salt Typhoon's targets were located in that region."* Discovered in 2023 *"Salt Typhoon is the cyber-spy gang that hacked telecommunications and government agencies to gain stealthy, long-term access to victim organizations going back as far as 2019. ... ESET's malware hunters found the group's new backdoor, called SparroWocky, deployed against government agencies in Argentina, Ecuador, Guatemala, Honduras, Panama, Peru, Puerto Rico, and Venezuela."*⁷

10. Assessment: Like Russia, cyber campaigns from the People's Republic of China frequently blend criminal with government, cyber-crime with cyber-espionage. The PRC plays a longer strategic approach than Russia as demonstrated by the shift in 'Salt Typhoons' targeting. Our previous reports have shown the PRC has also introduced AI to its hackers. The attack on retailers (paragraph 8) demonstrates how AI is being progressively integrated into its cyber operations. Although that report identified a single hacker, like Russia, the PRC is also using government hacking teams, companies, criminal hackers, and individuals in its operation. The 'ramp up' of AI may be relatively slower and more deliberate than Russia, however it is occurring.

Iran

11. Iranian Spies Using 'Chosen Brick' Malware. The FBI, UK National Cyber Security Centre, and the Netherlands' General Intelligence and Security Service (AIVD) are warning that *"Iranian state cyber actors are targeting individuals using social messaging apps to deploy surveillance and data-stealing malware on their Windows machines. ... Iran almost certainly uses cyber activity to support the repression of individuals who are seen as a threat to the regime, such as dissidents, activists and journalists, ... In some cases, the Iranian intelligence services have plotted to kidnap or conduct lethal operations against individuals internationally, who they perceive as enemies of the regime."* The attacks start with extensive research of the targets. *"These attacks typically begin with WhatsApp and Telegram messages, purportedly coming from individuals and organizations that the victim knows and trusts."* Targets are asked to download and open a file, typically *"Pictory, RunwayML, Norton Antivirus, Telegram, Adobe Flash Player, and KeePass"* to name a few. The warning continues:

6 Source: The Register. [Crook used three open source agents to break into a Fortune 500 hospitality company, a major US airline and 25+ other orgs](#)

7 Source: The Register. [China's Salt Typhoon backdoors Latin American orgs with new snooping malware](#)



Cyber-Intelligence Report

*"this actor targets personal devices, not just corporate devices, organizations are recommended to circulate this with their staff that are likely to be targeted and support them in checking their personal devices too."*⁸

12. The attack cost approximately \$25.00 (USD) per target to run. *"at least 27 companies were compromised to varying degrees," Gambit says. The hackers stole information from over 600,000 unexpired credit cards from two of the compromised companies and injected skimmer scripts into five online stores. Additionally, they gained some access to a Fortune 500 hospitality company and to three US firms, including an airline, a private industrial supplies distributor, and an online fashion retailer."*⁹ Although the attacks were detected and countered by three organizations (Gambit AI Security, Cloudflare, and the Shadowserver foundation), *"researchers said the attacker repeatedly rebuilt the infrastructure and continued the attacks."*¹⁰

13. Other Iranian Cyber Attacks and Targets.

- In August, more than 100 internet exposed American water utilities were targeted. This included *"two private water utilities in Colorado"*. Disruptions were described as *"brief and did not affect water services or public safety."*¹¹
- Also in August: Iran shut down a small UK power plant.
- Also in August: Iran used *"AI-generated exploitation scripts to break into internet-exposed Siemens S7 Series programmable logic controllers (PLCs) at water, manufacturing, energy, and other critical facilities."* This attack is ongoing.
- There have been at least three known cyber attacks on oil and gas tankers by Iranian hackers. According to 'gCaptain', the first two ships were a bulk oil carrier and the second a *"liquefied natural gas carrier"* or LNG.¹²

14. Assessment: Iranian Cyber Attacks. So far, cyber attacks from Iran and associated proxies have been largely ineffective. The 'Chosen Brick' campaign supports Iranian intelligence conducting kidnapping or potentially killing targets. Although very difficult to do, the attack on the LNG carrier has the potential to cause a catastrophic fire. The feeding of data to Iranian Intelligence strongly indicates their intent is to cause grave or lethal damage. These attacks must not be ignored.

This cyber-intelligence product is produced by David Swan. It is copyright David Swan 2026. This report is **TLP:CLEAR**¹³ and MAY be shared freely.

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

8 Source: The Register. [Iranian spies hit Windows machines with Chosen Brick data-stealing malware](#)

9 Source: Security Week. [AI-Powered Campaign Targets Hundreds of Online Retailers](#)

10 Source: Computing.co.uk. [AI agents used to steal hundreds of thousands of credit card records](#)

11 Source: Security Week. [Colorado Water Utilities Hit by Cyberattacks Targeting OT Systems](#)

12 Source: gCaptain. [US Coast Guard and FBI Conduct Cyberattack Probes on Tankers](#)

13 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.