

СПЕЦИАЛИЗИРАНИ ЗЛОВРЕДНИ СОФТУЕРИ ЗА ОПЕРАТИВНИ ТЕХНОЛОГИИ И СТРАТЕГИЧЕСКОТО СЪРЕВНОВАНИЕ В КИБЕРПРОСТРАНСТВОТО

ас. Димитър Събев Димитров

Висше военноморско училище „Н. Й. Вапцаров“ – Варна

E-mail: ds.dimitrov@naval-acad.bg

Резюме: *Статията представя обзор на развитието на специализираните зловредни софтуери, насочени към оперативните технологии и индустриалните системи за управление, и анализира неговото значение в условията на стратегическо съревнование в киберпространството. Разгледани са Stuxnet, Industroyer, Triton/Trisis, Industroyer2, Pipedream/Incontroller и FrostyGoop като последователни етапи в прехода от компрометиране на информационни системи към целенасочено въздействие върху физически процеси.*

Ключови думи: *оперативни технологии, зловредни софтуери, стратегическо съревнование.*

SPECIALIZED MALWARE FOR OPERATIONAL TECHNOLOGY AND STRATEGIC COMPETITION IN CYBERSPACE

Assist. Dimitar S. Dimitrov

Nikola Vaptsarov Naval Academy – Varna

E-mail: ds.dimitrov@naval-acad.bg

Abstract: *The article provides an overview of the evolution of specialized malware targeting operational technologies (OT) and industrial control systems (ICS) and analyzes its significance in the context of strategic competition in cyberspace. Stuxnet, Industroyer, Triton/Trisis, Industroyer2, Pipedream/Incontroller, and FrostyGoop are examined as successive stages in the transition from the compromise of information systems to targeted effects on physical processes.*

Keywords: *operational technologies, malware, strategic competition.*

1. ВЪВЕДЕНИЕ

Дигитализацията на енергетиката, производството, транспорта и комуналните услуги допринася за свързаността между информационните технологии и системите, които непосредствено управляват физически процеси. NIST определя оперативните технологии като програмируеми системи и устройства, които взаимодействат с физическата среда чрез наблюдение или пряко управление на процеси, събития и оборудване (Stouffer et al., 2023). Тази функционална връзка с физическия свят отличава ОТ от традиционните ИТ среди, а именно пробив в киберсигурността може да предизвика не само загуба на данни, но може и да доведе до прекъсване на производство, нарушаване на доставка на електроенергия, отпадане на защитни функции или други последствия за безопасността и обществото (Спасова, 2022).

В условията на стратегическо съревнование тази зависимост придобива значение, което надхвърля рамките на отделната организация. Стратегическата концепция на НАТО от 2022 г. определя киберпространството, критичната инфраструктура и устойчивостта като взаимосвързани елементи на колективната сигурност, като подчертава необходимостта от намаляване на стратегическите уязвимости и зависимостите (НАТО, 2022). Паралелно с това изследванията на киберкампаниите показват, че стратегическите резултати в киберпространството често се формират чрез продължителни серии от действия, а не само чрез единични високоефектни атаки (Harknett and Smeets, 2022).

Настоящата статия има обзореен характер и разглежда специализирания ОТ зловреден софтуер като технологичен израз на тази тенденция. Под „специализиран“ се разбира зловреден софтуер, чиито функции са създадени за взаимодействие с индустриални протоколи, контролери, инженерни системи или конкретна технологична логика. Този критерий е важен, защото подчертава факта, че не всяка кибератака срещу индустриална организация включва ОТ-специфичен код. Ransomware или стандартни средства за отдалечен достъп могат да прекъснат физически операции косвено, специализираният ОТ зловреден софтуер (Kamdzhlov and Nikolov, 2026), за разлика от тях, включва познание за самия индустриален процес и по този начин превръща кибердостъпа в инструмент за физическо въздействие.

2. ОПЕРАТИВНИТЕ ТЕХНОЛОГИИ КАТО СТРАТЕГИЧЕСКИ ОБЕКТ

Енергийните и индустриалните системи представляват кибер-физически архитектури, в които комуникационни мрежи, програмируеми контролери, релейни

защити, човеко-машинни интерфейси и физическо оборудване функционират като единна система. В електроенергетиката тази взаимозависимост е особено ясно изразена. Компрометиране на комуникационна или управляваща функция може да се пренесе към физическия процес, а локалният ефект да се разпространи чрез технологични зависимости. Поради това наличността, надеждността и безопасността имат приоритет, който ограничава възможността механично да се прилагат ИТ мерки без оценка на оперативния риск (Stouffer et al., 2023; Zografopoulos et al., 2021).

Стратегическото значение произтича и от ролята на критичната инфраструктура като поддържаща основа за държавното управление, икономиката, обществените услуги и военните способности. Електроснабдяването, комуникациите и транспортът не са изолирани сектори, а взаимнозависими функции. Следователно ОТ средата може да бъде разглеждана едновременно като техническа цел и като средство за генериране на вторичен ефект върху други системи. Това увеличава стойността на предварителното разузнаване, познаването на архитектурата и възможността за адаптиране на инструментите към конкретни индустриални протоколи (Николов, 2025).

ENISA поставя заплахите срещу наличността и ransomware сред водещите категории в европейската картина на заплахите, но при ОТ риска следва да се отчита допълнително възможността легитимни индустриални функции да бъдат използвани за злонамерено управление на процеса (ENISA, 2024). Именно тук специализираният ОТ зловреден софтуер се различава от масовия зловреден софтуер в това, че неговият ефект се основава на познаване на технологичната среда, а не само на компрометиране на операционна система.

3. ЕВОЛЮЦИЯ НА СПЕЦИАЛИЗИРАНИЯ ЗЛОВРЕДЕН СОФТУЕР ЗА ОТ

Stuxnet се приема като повратна точка, поради факта, че демонстрира възможност зловреден код да манипулира програмируеми контролери и чрез промяна на индустриална логика да влияе върху физически процес. Анализът на Langner подчертава, че целта не е традиционно информационно въздействие, а физическо изменение на поведението на индустриалната система (Langner, 2011; Andreev and Dimitrov, 2021). От стратегическа гледна точка Stuxnet показва, че специфичното инженерно знание може да бъде превърнато в софтуерна способност, способна да действа скрито в кибер-физическа среда.

Следващ важен етап е украинският електроенергиен сектор. Атаката от 2015 г. използва комбинация от стандартни ИТ инструменти, придобити идентификационни данни и ръчно управление на операторски системи. Година по-късно Industroyer автоматизира част от това познание. ESET установява модули за IEC 60870-5-101, IEC

60870-5-104, IEC 61850 и OPC DA – протоколи, използвани при управление на електроенергийни процеси (Savarro et al., 2026). Това е съществен преход: вместо операторът да изпълнява всяко действие ръчно, част от логиката за взаимодействие с подстанционната инфраструктура е кодирана в malware framework.

Triton/trisis разширява модела към системите за безопасност (Aanonsen, 2025). При инцидента от 2017 г. зловредният софтуер е създаден за взаимодействие с Triconex Safety Instrumented System контролери. Mandiant оценява, че нападателят е развивал способност за въздействие върху защитни функции, чието предназначение е да приведат индустриалния процес в безопасно състояние (Miller et al., 2021). Тук стратегическият риск е по-висок не заради мащаба на конкретния инцидент, а защото компрометирането на независим слой за безопасност може да промени границата между кибернарушение и физически опасно състояние.

През 2022 г. Industroyer2 потвърждава, че вече позната ОТ-специфична кодова база може да бъде приспособена към нова цел. ESET и Mandiant описват варианта като самостоятелен Windows executable, ограничен до IEC 60870-5-104 и снабден с вградена конфигурация за конкретни устройства и параметри на целевата среда (ESET Research, 2022; Kapellmann Zafra et al., 2022). Значението на случая е в повторната употреба на концепция, анализирана публично в продължение на години. Това показва, че разкриването на дадена ОТ способност не обезсмисля непременно нейната бъдеща оперативна стойност (Nikolov, 2026).

Година	Заплаха	ОТ/ICS специфика	Стратегическо значение
2010	Stuxnet	Манипулиране на PLC логика и физически процес	Кодира инженерно знание за конкретна технологична цел
2016	Industroyer	IEC-101/104, IEC 61850, OPC DA	Автоматизира управление на електроенергийно оборудване
2017	TRITON/TRISIS	Triconex SIS / TriStation	Поставя под риск независимия слой за безопасност
2022	Industroyer2	Самостоятелен IEC-104 компонент с целева конфигурация	Показва повторна употреба и адаптация на известна ОТ способност
2022	PIPEDREAM / INCONTROLLER	OPC UA, Modbus, CODESYS и индустриални устройства	Модулна, междусекторна и мащабируема атакуваща рамка
2024	FrostyGoop	Modbus TCP команди към индустриални контролери	Демонстрира физически ефект чрез легитимна протоколна функционалност

Таблица 1. Ключови етапи в развитието на специализирания ОТ зловреден софтуер.

Същата година pipedream/incontroller демонстрира друга тенденция - преминаване към по-модулни и междусекторни възможности. Съвместното съобщение на CISA, DOE, NSA и FBI описва инструменти, способни да взаимодействат с широко използвани ICS/SCADA устройства и технологии, включително OPC UA, Modbus и CODESYS (CISA et al., 2022; Dimitrov and Andreev, 2025). За разлика от инструмент, проектиран за един конкретен обект, такава архитектура може да намали необходимостта от разработване на изцяло нов зловреден софтуер за всеки бъдещ сценарий.

FrostyGoop от 2024 г. допълва предходните атаки с по-улеснен, но стратегически важен модел. Dragos описва Windows базиран зловреден софтуер, който използва стандартни Modbus TCP команди за четене и запис на стойности в контролери. свързан инцидент срещу районна топлофикационна компания в Украйна води до загуба на отопление за над 600 жилищни сгради за почти два дни (Dragos, 2024). Случаят показва, че високо въздействие не изисква задължително сложна експлоатация на неизвестни уязвимости. При достатъчен достъп нападателят може да използва легитимните функции на индустриалния протокол с враждебно предназначение.

4. ОТ ЗЛОВРЕДЕН СОФТУЕР И СТРАТЕГИЧЕСКОТО СЪРЕВНОВАНИЕ В КИБЕРПРОСТРАНСТВОТО

От прегледаните случаи могат да бъдат изведени три взаимосвързани характеристики. Първата е систематизирането на експертно знание. Специализираният зловреден софтуер превръща познания за протоколи, устройства и последователности на управление в изпълнима логика. Това намалява зависимостта от ръчно действие в момента на атаката и може да увеличи скоростта и повторемостта на въздействието.

Втората характеристика е предварителната подготовка. Конфигурации за конкретни устройства, IOA адреси, контролери или защитни системи предполагат предходно разузнаване на средата. Така реалната стойност на една кибероперация не започва с изпълнението на destructive payload, а с натрупването на техническо знание и достъп.

Третата характеристика е потенциалът за стратегическа сигнализация и принуда, дори когато разрушителният компонент не е използван. Разкритият pipedream е пример за разработена способност без публично потвърден успешен разрушителен инцидент при първоначалното му оповестяване. От аналитична гледна точка наличието на

подобен инструмент разширява набора от възможни действия при бъдеща криза. Това не доказва конкретно политическо намерение, но показва защо техническите способности следва да се оценяват като част от по-широката стратегическа среда.

В този смисъл ОТ зловредния софтуер функционира като връзка между киберкампанията и физическия ефект. Harknett и Smeets разглеждат киберкампаниите като продължителна форма на взаимодействие, чрез която участниците преследват стратегически резултати във времето (Harknett and Smeets, 2022). При критичната инфраструктура тази динамика включва проникване, картографиране на зависимости, поддържане на достъп, разработване или адаптиране на инструменти и едва след това непосредствено въздействие. Следователно защитата не може да бъде ориентирана единствено към финалния разрушителен етап.

Допълнителен проблем е двойственият характер на много индустриални функции. Modbus, IEC-104 или инженерните интерфейси са легитимни механизми за управление, злонамерената употреба може да изглежда синтактично коректна, но да е неправилна спрямо нормалното състояние на процеса. Поради това разграничаването между нормална и враждебна активност изисква контекст за ролите на устройствата, допустимите команди, времевите зависимости и физическите ограничения. Тази особеност обяснява защо ОТ защитата се нуждае от процесно ориентирано наблюдение и не може да разчита само на класически индикатори за компрометиране (Nikolov and Nikolov, 2024; Chagovet et al., 2026)).

5. ЗАКЛЮЧЕНИЕ

Специализираният зловреден софтуер за оперативни технологии представлява сравнително ограничена по брой, но стратегически значима категория киберспособности. От Stuxnet до FrostyGoop се проследява последователно натрупване на модели за взаимодействие с физически процеси: кодиране на инженерно знание, автоматизиране на индустриални протоколи, насочване към системи за безопасност, повторна употреба на вече разкрити способности, изграждане на междусекторни рамки и злоупотреба с легитимни протоколни функции.

Тези развития показват, че основният риск не се изчерпва с отделния отпечатък на зловредния софтуер. Стратегическата стойност се формира от съчетанието между достъп, разузнаване на средата, техническо познание и възможност за превръщане на цифровото действие във физически ефект. Поради това ОТ киберсигурността трябва да

бъде интегрирана в по-широки политики за устойчивост на критичната инфраструктура. За държавите и организациите ключовият въпрос не е единствено как да бъде открит конкретен зловреден инструмент, а как да се ограничи способността на противника да натрупа, поддържа и използва оперативно знание за критичните технологични процеси.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

- CISA, DOE, NSA, FBI. 2022. APT Cyber Tools Targeting ICS/SCADA Devices. Joint Cybersecurity Advisory AA22-103A. Available from: https://www.cisa.gov/sites/default/files/publications/AA22-103A_APT_Cyber_Tools_Targeting_ICS_SCADA_Devices.pdf. [viewed 06.10.2026].
- DRAGOS. 2024. How to Protect Against FrostyGoop: ICS Malware Targeting Operational Technology. 23 July 2024. Available from: <https://www.dragos.com/blog/protect-against-frostygoop-ics-malware-targeting-operational-technology>. [viewed 06.10.2026].
- DIMITROV, D., E. ANDREEV. 2025. China's Strategic Competition in Cyberspace: Volt Typhoon and Salt Typhoon as a Projection of Power, a More Aggressive Posture and a Future Beyond Espionage. – In: Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference. Rezekne: RTU Press, Vol. 2, pp. 115 – 122. ISSN 2256-070X. DOI: 10.17770/etr2025vol2.8618.
- ENISA. 2024. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. Available from: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>. [viewed 06.10.2026].
- SAVARRO, D., M. BORRELLI, E. G. AMPARORE, D. CEROTTI, G. FRANCESCHINIS, S. DONATELLI. 2026. Predictive and Diagnostic Inference for Power Systems Cybersecurity: Analysis of the Industroyer Cyber-Kill Chain. – In: Computer Performance Engineering: 22nd European Workshop on Performance Engineering (EPEW 2026). Berlin, Heidelberg: Springer-Verlag, pp. 51–65. DOI: 10.1007/978-3-032-29105-9_4.
- ESET RESEARCH. 2022. Industroyer2: Industroyer Reloaded. 12 April 2022. Available from: <https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/>. [viewed 06.10.2026].
- HARKNETT, R. J., M. SMEETS. 2022. Cyber campaigns and strategic outcomes. – In: Journal of Strategic Studies. Vol. 45, No. 4, pp. 534 – 567. DOI: 10.1080/01402390.2020.1732354.

- AANONSEN, C. E. 2025. Stuxnet, Revisited (Again): Producing the Strategic Relevance of Cyber Operations. – In: Journal of Cyber Policy. Vol. 10, No. 1, pp. 68–84. DOI: 10.1080/23738871.2025.2492570.
- KAMDZHALOV, S., D. NIKOLOV. CYBER THREAT INTELLIGENCE BASED SCOPING OF RED TEAM EXERCISES. – In: SysTechDev. 2026, vol. 3, pp. 115 – 119. DOI: 10.68302/std2026.vol3.210.
- LANGNER, R. 2011. Stuxnet: Dissecting a Cyberwarfare Weapon. – In: IEEE Security & Privacy. Vol. 9, No. 3, pp. 49 – 51. DOI: 10.1109/MSP.2011.67.
- MILLER, T., A. STAVES, S. MAESSCHALCK, M. STURDEE, B. GREEN. 2021. Looking Back to Look Forward: Lessons Learnt from Cyber-Attacks on Industrial Control Systems. – In: International Journal of Critical Infrastructure Protection. Vol. 35, Article 100464. DOI: 10.1016/j.ijcip.2021.100464.
- NATO. 2022. NATO 2022 Strategic Concept. Brussels: North Atlantic Treaty Organization. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf. [viewed 06.10.2026].
- NIKOLOV, B., D. NIKOLOV. A Scenario-based Approach to Cybersecurity Training for Seafarers. – In: 24th International Association of Maritime Universities (IAMU) Conference. Massachusetts Maritime Academy, USA, 2024, pp. 385 – 390. ISSN 2706-6762.
- NIKOLOV, D. DCSYNC ATTACK FROM AN ADVERSARY POINT OF VIEW. – In: SysTechDev. 2026, vol. 3, pp. 219 – 222. DOI: 10.68302/std2026.vol3.213.
- STOUFFER, K. et al. 2023. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-82r3.
- ZOGRAFOPOULOS, I., J. OSPINA, X. LIU, C. KONSTANTINOU. 2021. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. – In: IEEE Access. Vol. 9, pp. 29775 – 29818. DOI: 10.1109/ACCESS.2021.3058403.
- НИКОЛОВ, Д. Анализ на планирането и изпълнението на киберупражнения. – В: Девета международна научна конференция Радиационната безопасност в съвременния свят. 2025, с. 146 – 158. ISSN 2738-7607. COBISS.BG-ID 48925192.
- СПАСОВА, В. 2022. Сигурност по дизайн в софтуерното инженерство. Монография. Варна: ВСУ „Черноризец Храбър“. ISBN 978-954-715-834-7.