



Intelligence Games in the Power Grid

Deception-Denial-Manipulation

Jeff Bardin – Treadstone 71

jbardin@treadstone71.com



Outline

Russian Views and Values – Russian Cyber Program (Cyber and Physical)

Possible Hypotheses

Delta Electronics

Oleg Strekozov

The Matrix Group

Yuri Chekunov

BlackEnergy

Analysis

Russian company imitating Taiwanese firm.

Taiwanese firm linked from Russian firm pointing to software that is infected without (Deltaww) knowing.

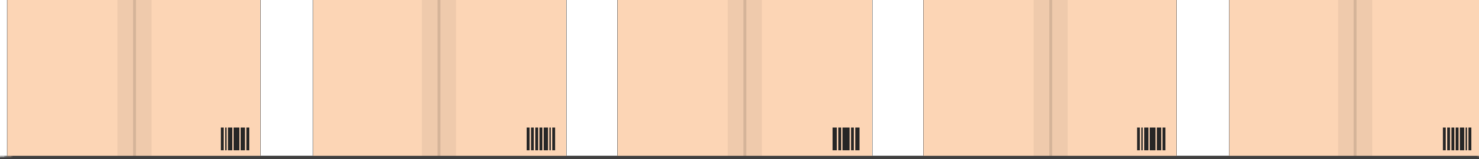
Malware aligns with a certain APT.

Russian oligarchs involved in SCADA equipment buying and selling.

Hybrid warfare intent for later issues associated with energy firms potentially to artificially push oil prices higher when required.



Russian Views - Values



Cyber operations part of information warfare NOT seen as a separate function or command.



The use of information in Western countries to manipulate public opinion is a core function of hybrid warfare



The expansion of NATO, potential addition of new EU countries to NATO, Western troops in Afghanistan, are a clear and present danger to Russia.

Russians think geopolitically and physically with emphasis on their periphery.



Any voices of dissent, internal or external, are identified and targeted as threats.



Corruption is a mainstay and a required value providing monetary value to leadership and demonstrating loyalty



USA, NATO, allies—Georgia, the Ukraine, and Estonia—are (obviously) threats.



“First and foremost it is worth acknowledging that the demise of the Soviet Union was the greatest geopolitical catastrophe of the century”





The Russian Cyber Program



Federal Agency of Government



ral Protective Service of Russia



eral Security Service of Russian Federation



Russian Interior Ministry's K Directorate



Youth Democratic Anti-Fascist Movement - NASHI



РОСКОМНАÐ3ОР

The Ministry of Communications and Mass Media (Minkomsvyaz)



Trolls of Olgino



- as-rbncus(member of as-sbtel)
- Credolink ASN Credolink ISP Autonomous System St Petersburg
- AKIMON AS Aki Mon Telecom
- CONNECTCOM ConnectCom Ltd Autonomous System
- DELTASYS Delta Systems network
- RBN AS Russian Business Network
- OINVEST AS Online Invest group LLC
- SBT AS SBT Telecom
- RUSTELECOM AS Rustelecom AS
- MICRONNET AS Micronnet LTD
- NEVSKCC AS NEVACON LTD



Cyber and Physical Intersection - Russia

• Cyber Adversaries

- APT28 Fancy Bear
- APT29 The Dukes
- Energetic Bear
- Sandworm Team
- Turla Group

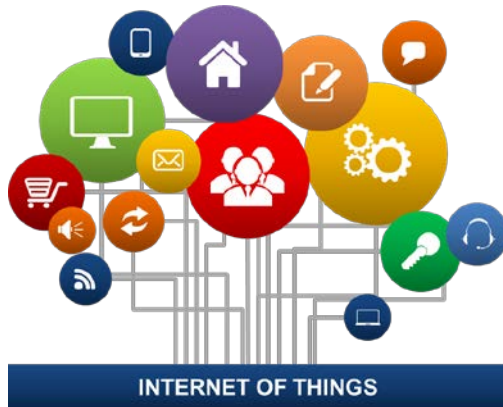
• Physical Adversaries

- Delta Electronics
- Matrix Group LLC
- Spektrum Elektro Servis
- Centropas-Yugoriya
- Civil Protection Department of the Population of Khanty-Mansi Autonomous District - Yugra





Possible Hypotheses



A good hypothesis meets the following criteria:

- Is testable and falsifiable.
- Is written as a definite statement, not as a question.
- Is based on observations and knowledge.
- Predicts the anticipated results clearly.
- Contains a dependent and an independent variable—a “what” and a “why.” The dependent variable is the phenomenon being explained, and the independent variable does the explaining.

Hypothesis One

Delta Elektronik is a legitimate reseller of Delta Electronics Taiwan hardware in business for profit.

Hypothesis Two

Delta Elektronik is a fake company set up by a nation state in collusion with criminal elements in order to generate revenue and launder money.

Hypothesis Three

Delta Elektronik is a fake company established with the support of the government used to sell legitimate SCADA hardware with malware backdoors in the PLC software for later exploitation.

Hypothesis Four

Delta Elektronik is a front company used by Russian intelligence/nation state actors and oligarchs to infect energy organizations for present day cyber espionage and targeted sabotage while generating money for oligarchs.

Hypothesis Five

Delta Elektronik is a front company used by a criminal group to either defraud energy companies by providing fraudulent equipment or skim off the top.



Possible Hypotheses

Hypothesis Six

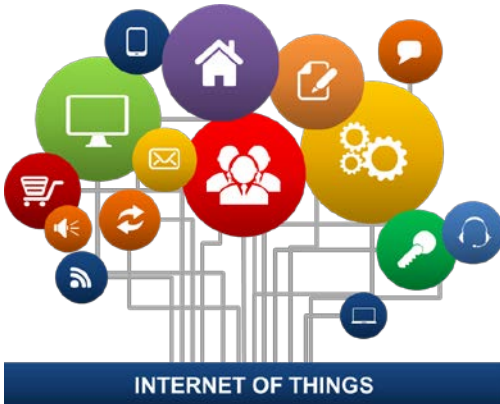
Energetic Bear started after learning about PLCs from Delta Elektronics as part of a Russian hybrid warfare program and is now fully integrated with Delta Elektronics in a physical/cyber focused effort.

Hypothesis Seven

Energetic Bear performs full-scope cyber operations from reconnaissance and data collection, intelligence production and analysis, software obfuscation, infection, modification, and expansion as part of the Russian government's hybrid warfare efforts used to destabilize hostile regimes.

Hypothesis Eight

Energetic Bear is a criminal enterprise operating at the periphery of the Russian government for monetary gain.





Delta Electronics - Taiwan



Solutions Products News Center Investor Services About Delta Careers

Regions | Language

Google Custom Q



CSR Role Model to Global Corporate Citizen

Delta continuously focuses on climate change and energy conservation that coincide with global sustainable development goals. We won 3 major awards at Global Views Monthly's 13th annual "Global Views CSR Awards" event, receiving the most awards among all awarded companies while setting benchmarks in the electronics industry

Our Business

Power Electronics

- Component
- Embedded Power
- Fan & Thermal Management
- Automotive Electronics
- Merchant & Mobile Power



Automation

- Industrial Automation
- Building Automation

Infrastructure

- ICT Infrastructure
- Energy Infrastructure

Solutions

- Industrial Automation Solutions
- Building Automation Solutions
- Datacenter Solutions
- Telecom Power Solutions
- Renewable Energy Solutions
- Display and Monitoring Solutions
- EV Charging Solutions



Features



Delta Electronics Wins Three Major Awards at the 2017 Global Views Monthly's CSR Awards
14 awards won since 2005 – the most by one company since the founding of the awards

News

- 2017/05/10 - Delta Electronics' Consolidated Sales Revenues for April 2017 Totaled NT\$17,493 Million
- 2017/04/27 - Delta Electronics Announces 1Q 2017 Financial Results



Delta Electronics - Russia



[Контакты](#) [Новости](#) [Сертификаты](#) [Delta Electronics, Inc](#)

Телефон : +7 (495) 984-51-05 (Москва), +7 (812) 640-46-90 (Санкт-Петербург), E-mail: info@delta-electronics.info, Время работы: 9-18.



- ✓ [Ваш заказ \(корзина\)](#)
- ✓ [Каталог](#)

- ▶ [Преобразователи частоты](#)
- ▶ [Сервоприводы](#)
- ▶ [Системы ЧПУ](#)
- ▶ [Программируемые контроллеры](#)
- ▶ [Панели оператора](#)
- ▶ [Текстовые панели](#)
- ▶ [Температурные контроллеры](#)
- ▶ [Счетчики и таймеры](#)
- ▶ [Энкодеры](#)
- ▶ [Коммуникационные модули](#)
- ▶ [Ethernet Switches](#)
- ▶ [Источники питания](#)
- ▶ [Приборы и Датчики](#)

Каталог

▶ Промышленная автоматизация Дельта Электроникс



Наши знания и опыт в автоматизации управления производством мы фокусируем в следующих видах продукции:

Преобразователи частоты



Сервоприводы



[Для прецизионного](#)

Системы ЧПУ



[Системы числового](#)

Энкодеры





Delta Electronics

Registrations by Oleg Strekozov:

- AVTOPAK-VOLGA (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU AVTOPAK-VOLGA, TIN: 6319701227, address: 443109, g Samara, ul Tovarnaya, d 8)
- Ayut (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU Ayut, TIN: 7720692855, address: 111395, g Moscow, ul Moldagulovoj, d 10, korp 1, ofis 20)
- IntelGrupp (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU IntelGrupp, TIN: 7719757272, address: 105275, g Moscow, ul Borisa ZHigulenkova, d 21 A, ofis 60)
- Misteriya (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU Misteriya, TIN: 7707733809, address: 127473, g Moscow, ul Delegatskaya, d 3, str 5)
- NIKS (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU NIKS, TIN: 7728747658, address: 117133, g Moscow, ul Akademika Vargi, d 40 A)
- Prima (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU Prima, TIN: 7706743265, address: 119017, g Moscow, ul Bolshaya Ordinka, d 40, str 7)
- TDSaturn (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU TDSaturn, TIN: 7707733848, address: 127473, g Moscow, ul Delegatskaya, d 3, str 3)
- Tekstiltorg (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU Tekstiltorg, TIN: 7725702200, address: 115280, g Moscow, ul Leninskaya Sloboda, d 23, ofis 5)
- Emilina (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU Emilina, TIN: 7714814618, address: 125040, g Moscow, ul Raskovoj, d 1, ofis 63)
- Magnum (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU Magnum, TIN: 7705930382, address: 115184, g Moscow, ul Bahrushina, d 1, str 2)
- Rakurs (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU Rakurs, TIN: 7733771014, address: 125430, g Moscow, ul Mitinskaya, d 52, korp 2, ofis 13)
- Nyu-Lajn (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU Nyu-Lajn, TIN: 7713731528, address: 127474, g Moscow, bulv Beskudnikovskij, d 11, korp 3 A)
- StrojHolding (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU StrojHolding, TIN: 7724804136, address: 115409, g Moscow, ul Koshkina, d 5, str 8)
- EkonomMarket (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU EkonomMarket, TIN: 7731412490, address: 121609, g Moscow, bulv Osennij, d 5, korp 3)
- MTK (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU MTK, TIN: 5027181836, address: 140000, Moskovskaya area, g Lyubertci, ul Volkovskaya, d 43)
- Inrost (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU Inrost, TIN: 5038092948, address: 141206, Moskovskaya area, g Pushkino, Kudrinskoe shosse, d 3)
- Delta Elektroniks (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU Delta Elektroniks, TIN: 5001090038, address: 143903, Moskovskaya area, g Balashiha, ul Vladimirskaaya, d 139)
- Vintazh (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU Vintazh, TIN: 5027193398, address: 140006, Moskovskaya area, g Lyubertci, ul YUzhnaya, d 26 A)





Oleg Strekozov

195.88.209.6 has been listed on Cyberwarzone because it has a history of malicious activities. The IP has been reported on various domains which keep track of malicious IP's. The chance is very high that 195.88.209.6 has already been added to your blacklist service provider.

Reasons why 195.88.209.6 is listed on Cyberwarzone:

- History of being on a blacklist
- History of being used in an aggressive marketing campaign
- History of malicious traffic or use
- Triggered as a spam-bot or aggressive crawler
- We were lazy and we did not see that it is a false-positive

Information on the IP

In the table below you will be able to view information which is related to the IP address which is mentioned above.

IP Address	195.88.209.6
Country	Russian Federation
Network Name	IPSERVER
From IP	195.88.208.0
To IP	195.88.209.255
Classless Inter-Domain Routing (CIDR)	195.88.208.0/23

Owner name	Antaro Ltd.
Contact name	Strekozov Oleg Vladimirovich
Address	Russia, 107031, Moscow, proezd Dmitrovskiy 8
E-mail	
Abuse email	abuse@ipserver.su



Delta Electronics - Registrations

- OOO "DELTA-ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "DELTA-ELEKTRONIKS", TIN: 7731273670, address: G Moscow,UL MOLODOGVARDEJSKAYA, D 57, STR 3)
- OOO "DELTA ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "DELTA ELEKTRONIKS", TIN: 5012019982, address: MOSKOVSKAYA AREA,G ZHELEZNODOROZHNIJ,UL 1 MAYA, D 16)
- OOO "DELTA ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "DELTA ELEKTRONIKS", TIN: 4501112440, address: 640000, G KURGAN, UL K MARKSA, D 40, KV 13)
- OOO "DELTA ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "DELTA ELEKTRONIKS", TIN: 7733578268, address: 125373, G Moscow, BULV YANA RAJNISA, D 30, KORP 1)
- OOO "DELTA-ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "DELTA-ELEKTRONIKS", TIN: 7709829111, address: 109004, G Moscow, PER PESTOVSKIJ, D 10, STR 1)
- OOO "Delta Elektroniks" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "Delta Elektroniks", TIN: 7718767630, address: 107392, g Moscow, ul Prostornaya, d 7, str 1, ofis 309)
- OOO "Delta Elektroniks" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "Delta Elektroniks", TIN: 7842414541, address: 191014, G St.Petersburg, PER SOLDATSKIJ, 6 LITER A POM 12-N)
- OOO "DELTA ELEKTRONIKS" (Likvidatcionnaya komissiya OOO "DELTA ELEKTRONIKS" (reshenii o likvidacii i o likvidatcionnoj komissii), TIN: 7716703381, address: 111024, g Moscow, ul Aviamotornaya, d 50, str 2, pom XI, komn 10)
- OOO "Delta Elektroniks" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "Delta Elektroniks", TIN: 5001090038, address: 143903, Moskovskaya OBL, Balashiha G, Vladimirskaia UL, 139)
- OOO "DELTA ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "DELTA ELEKTRONIKS", TIN: 7806516146, address: 195027, g St.Petersburg, rajon Krasnogvardejskij, munitcipalnij region Bolshaya Ohta, PROSP SHAUMYANA, 4 KORP 1 LITER A)
- OOO "DELTA-ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "DELTA-ELEKTRONIKS", TIN: 5003113629, address: 142715, Moskovskaya area, Leninskij rajon, Kartinskij selskij region, PR PROMISHLENNIJ, D 9)
- OOO "DELTA ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "DELTA ELEKTRONIKS", TIN: 6658037829, address: 620028, G EKATERINBURG,UL DOLORES IBARRURI D 2 K 1)

Org-info.com



Delta Electronics - Registrations

Evtuyhin Oleg Vladimirovich

OOO "NEOLAJT" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "NEOLAJT", TIN: 7722507360, address: 109052, G Moscow, UL PODEMNAYA, D 7)

OOO "MIRAZH" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "MIRAZH", TIN: 7722507346, address: 109052, G Moscow, UL PODEMNAYA, D 7)

OOO "DELTA-ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "DELTA-ELEKTRONIKS", TIN: 7731273670, address: G Moscow, UL MOLODOGVARDEJSKAYA, D 57, STR 3)

OOO "TRANSGAZREZERV +" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "TRANSGAZREZERV +", TIN: 7734258503, address: 123098, g Moscow, Severo-Zapadnij administrativnij region, rajon Horoshevo-Mnevniki, UL ZHIVOPISNAYA, D 21, KORP 4)

OOO "STEKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "STEKS", TIN: 7722293060, address: 109052, G Moscow, UL POD'EMNAYA, D 14, STR 1)

OOO "STROJSERVIS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "STROJSERVIS", TIN: 7722507378, address: 109052, g Moscow, ul Pod_emnaya, d 7)

OOO "NORDIS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "NORDIS", TIN: 7722507385, address: 109052, G Moscow, UL PODEMNAYA, D 7)

OOO "LIANA" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "LIANA", TIN: 7722507353, address: 109052, G Moscow, UL PODEMNAYA, D 7)

OOO "FIERA" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "FIERA", TIN: 7705585425, address: 113054, G Moscow, UL VALOVAYA, D 30/73, STR 4)

OOO "FINANSOVAYA I YURIDICHESKAYA EKSPERTIZA" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "FINANSOVAYA I YURIDICHESKAYA EKSPERTIZA", TIN: 7702527390, address: 129041, G Moscow, PROSP MIRA, D 52, STR 5)



Delta Electronics - Registrations

OOO "DELTA-ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "Delta Elektroniks", TIN: 7718767630, address: 107392, g Moscow, UL MOLODOGVARDEJSKAYA, D 57, STR 3)

OOO "DELTA ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "Delta Elektroniks", TIN: 7842414541, address: 191014, G MOSKOVSKAYA AREA, G ZHELEZNODOROZHNIJ, UL 1 MAYA)

OOO "DELTA ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "Delta Elektroniks", TIN: 5001090038, address: 143903, G KURGAN, UL K MARKSA, D 40, KV 13)

OOO "DELTA ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "Delta Elektroniks", TIN: 7806516146, address: 195027, G Moscow, BULV YANA RAJNISA, D 30, KORP 1)

OOO "DELTA-ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "Delta Elektroniks", TIN: 6658037829, address: 620028, G Moscow, PER PESTOVSKIJ, D 10, STR 1)

OOO "Delta Elektroniks" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "Delta Elektroniks", TIN: 7718767630, address: 107392, g Moscow, ul Prostornaya, d 7, str 1, ofis 309)

OOO "Delta Elektroniks" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "Delta Elektroniks", TIN: 7842414541, address: 191014, G St.Petersburg, PER SOLDATSKIJ, 6 LITER A POM 12-N)

OOO "DELTA ELEKTRONIKS" (Likvidatsionnaya komissiya OOO "DELTA ELEKTRONIKS" (reshenii o likvidatsii i o likvidatsionnoj komissii), TIN: 7716703381, address: 111024, g Moscow, ul Aviamotornaya, d 50, str 2, pom XI, komn 10)

OOO "Delta Elektroniks" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "Delta Elektroniks", TIN: 5001090038, address: 143903, Moskovskaya OBL, Balashiha G, Vladimirskaia UL, 139)

OOO "DELTA ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "DELTA ELEKTRONIKS", TIN: 7806516146, address: 195027, g St.Petersburg, rajon Krasnogvardejskij, munitcipalnij region Bolshaya Ohta, PROSP SHAUMYANA, 4 KORP 1 LITER A)

OOO "DELTA-ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "DELTA-ELEKTRONIKS", TIN: 5003113629, address: 142715, Moskovskaya area, Leninskij rajon, Kartinskij selskij region, PR PROMISHLENNIJ, D 9)

OOO "DELTA ELEKTRONIKS" (OBSHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU "DELTA ELEKTRONIKS", TIN: 6658037829, address: 620028, G EKATERINBURG, UL DOLORES IBARRURI D 2 K 1)

Bogdanov Dmitrij YUrevich

SHumakov Sergej Aleksandrovich

Total number of organizations: 497

Zibin Aleksandr Anatolevich

Konstantinov Dmitrij Vladimirovich

Total number of organizations: 92



Matrix Group LLC

aucom.info
 autonic.su
 broen-ru.com
 china-drive.info
 control-techniques.com
 control-techniques.info
 danfoss-bauer.info
 danfoss-ru.com
 delta-electronics.biz
 deltaelectronics.info
 deltronic.info
 deltronic.su
 deltronics.info
 deltronix.info
 deltronix.su
 emotron-ru.com

fuji-ru.com
 hyundai-ru.com
 keb.su
 matrix-group.info
 matrix-group.su
 matrixgroup.info
 omron-hitachi.info
 optidrive.su
 privod.info
 prostar.su
 schneiderelectric.su
 tecorp.info
 toshiba-ru.com
 vacon-ru.com
 vesper-ru.com

The Matrix Group LLC lists over 260 domain names of varying legitimacy – owner of Delta Electronics – Russia – Assumption part of the

The screenshot shows the website for Matrix Group LLC, which is a product supply for Delta Electronics, Inc. The page features a navigation menu on the left with categories like 'Home', 'About Us', 'Products', and 'Services'. The main content area includes a header with the company name and logo, followed by a section titled 'Components Industrial Automation (Industrial Automation)'. Below this, there is a large image of a Delta Electronics product and a detailed description of the company's services and products. The right side of the page contains a sidebar with a search bar and a list of products, including 'Uninterruptible Power Supplies', 'Frequency Converters', and 'Temperature Controllers'. The footer includes contact information for Moscow and Saint-Petersburg, along with a phone number (8 800 555 90 55) and a 'TO CALL YOU BACK' button.

This screenshot shows a product page for 'UNINTERRUPTIBLE POWER SUPPLIES DELTA AMPLON | ULTRON | MODULON | AGULON'. The page features a large image of the power supply units and a list of 'ORDERING PRODUCTS' including 'Delta - Amplon', 'Delta - Ultron', and 'Delta - Modulon'. The page also includes a 'BASKET' section with a 'Total: 0' and a 'PRODUCT CATALOG' section. The footer contains contact information for Matrix Group LLC, including phone numbers for Moscow and Saint-Petersburg, and a 'TO CALL YOU BACK' button. The page is part of a larger website structure, as indicated by the navigation menu at the top.



Custom search

Id	Type	URL
0	xls	http://www.delta-electronics.info/content/files/12_na_operatorskie_paneli_HMI_serii_TP_i_DOP_i_moduli_iz_rasshireniya.xls
1	xls	http://www.delta-electronics.info/content/files/11_na_isto4niki_besperebonogo_pitaniya_UPS.xls
2	xls	http://www.delta-electronics.info/content/files/2012_Pras_na_produkciju_DELTA_AuCom_Ehand_s_soderzaniem.xls
3	xls	http://www.delta-electronics.info/content/files/20091014_price_PLCDVP_i_iz_aksessuarov.xls
4	xls	http://www.delta-electronics.info/content/files/20090820_price_enkodery_DELTA.xls
5	xls	http://www.delta-electronics.info/content/files/20091110_Pras_na_servoprivoda_Delty.xls
6	xls	http://www.delta-electronics.info/content/files/20100301_Pras_servoprivod_DELTA.xls
7	xls	http://www.delta-electronics.info/userdata/files/20130828_Pras_na_produkciju_DELTA_s_soderzaniem.xls
8	xls	http://www.delta-electronics.info/userdata/files/20140520_Pras_list_ASD_Servoprivoda_DELTA_3.xls
9	xls	http://www.delta-electronics.info/content/files/11_na_servoprivoda_serii_ASDA_A_B_AB_A_V2.xls
10	xls	http://www.delta-electronics.info/content/files/11_na_operatorskie_paneli_HMI_serii_TP_i_DOP_i_moduli_iz_rasshireniya.xls
11	xls	http://www.delta-electronics.info/userdata/files/11_na_vrashayushiesya_opti4eskie_inkrementalnye_enkodery.xls
12	xls	http://www.delta-electronics.info/userdata/files/11_na_radio4astotnyye_filtry_dlya_preobrazovatele_4astoty_VFD.xls
13	xls	http://www.delta-electronics.info/userdata/files/12_na_temperaturnyye_kontrollery_DT_i_pribory_KIPIA.xls
14	xls	http://www.delta-electronics.info/content/files/13_na_servoprivoda_serii_ASDA_A2_V2.xls
15	xls	http://www.delta-electronics.info/content/files/12_na_preobrazovatele_4astoty_serii_VFD.xls
16	xls	http://www.delta-electronics.info/userdata/files/11_na_setevyye_drosseli_tipa_ED3N_2_kompanii_Ehand.xls
17	xls	http://www.delta-electronics.info/userdata/files/11_na_aksessuary_dlya_preobrazovatele_4astoty_VFD.xls
18	xls	http://www.delta-electronics.info/content/files/11_na_temperaturnyye_kontrollery_i_pribory_KIPIA.xls
19	xls	http://www.delta-electronics.info/userdata/files/11_na_motornyye_du_drosseli_tipa_ED3dU_kompanii_Ehand.xls
20	xls	http://www.delta-electronics.info/userdata/files/11_na_setevyye_drosseli_tipa_ED3N_4_kompanii_Ehand.xls
21	xls	http://www.delta-electronics.info/content/files/20091020_price_na_IP_DVPPS_DRP_PMC_DELTA.xls
22	xls	http://www.delta-electronics.info/userdata/files/11_na_motornyye_drosseli_tipa_ED3S_kompanii_Ehand.xls
23	xls	http://www.delta-electronics.info/content/files/20091012_price_HMI_DELTA_DOP-B05S101.xls
24	xls	http://www.delta-electronics.info/content/files/20090528_price_tom_aksessuary_VFD_BUE-20015.xls
25	xls	http://www.delta-electronics.info/content/files/20090615_price_aksessuary_VFD_kabeli_pulty_platy...xls
26	xls	http://www.delta-electronics.info/userdata/files/20081210_price_aksessuary_VFD-VL.xls
27	xlsx	http://www.delta-electronics.info/content/files/Pras_na_isto4niki_besperebonogo_pitaniya_UPS.xlsx
28	xlsx	http://www.delta-electronics.info/content/files/20170125_prais-list_PLCD_DELTA_i_aksessuarov.xlsx
29	xlsx	http://www.delta-electronics.info/userdata/files/20140901_Pras-list_VFD_DELTA.XLSX
30	pdf	http://www.delta-electronics.info/userdata/files/certificate_ASD_2012-2015.pdf
31	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
32	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf

Id	Type	URL
34	pdf	http://www.delta-electronics.info/userdata/files/Liniya_dlya_rezki_plyonki.pdf
35	pdf	http://www.delta-electronics.info/content/files/DVP_communication_Protocol_rus.pdf
36	pdf	http://www.delta-electronics.info/content/files/DVP_ES2_manual_rus.pdf
37	pdf	http://www.delta-electronics.info/content/files/DTA_manual_rus_DAE07.pdf
38	pdf	http://www.delta-electronics.info/content/files/TP_user_manual_rus.pdf
39	pdf	http://www.delta-electronics.info/content/files/DVP28SV_manual_rus.pdf
40	pdf	http://www.delta-electronics.info/content/files/BUE_manual_rus_bu00.pdf
41	pdf	http://www.delta-electronics.info/userdata/files/chocbuate.pdf
42	pdf	http://www.delta-electronics.info/content/files/VFDB4132_instruction_rus.pdf
43	pdf	http://www.delta-electronics.info/userdata/files/VFDEL_pump_application_rus.pdf
44	pdf	http://www.delta-electronics.info/content/files/Installation_Note_240W3PH_rus.pdf
45	pdf	http://www.delta-electronics.info/content/files/DTC_manual_rus_DCE3.pdf
46	pdf	http://www.delta-electronics.info/userdata/files/DOP_gabants.pdf
47	pdf	http://www.delta-electronics.info/content/files/Installation_Note_480W3PH_rus.pdf
48	pdf	http://www.delta-electronics.info/content/files/Installation_Note_240W1PH_rus.pdf
49	pdf	http://www.delta-electronics.info/content/files/Installation_Note_120W1PH_rus.pdf
50	pdf	http://www.delta-electronics.info/content/files/DTB_manual_rus_DBE4.pdf
51	pdf	http://www.delta-electronics.info/userdata/files/DTVFD_rus.pdf
52	pdf	http://www.delta-electronics.info/userdata/files/Zakyopo4naya_mashina.pdf
53	pdf	http://www.delta-electronics.info/content/files/DVP_EC3_manual_rus.pdf
54	pdf	http://www.delta-electronics.info/content/files/VFD_accessories_1.pdf
55	pdf	http://www.delta-electronics.info/content/files/DTD_manual_rus.pdf
56	pdf	http://www.delta-electronics.info/content/files/Braking_manual_rus_ue02.pdf
57	pdf	http://www.delta-electronics.info/content/files/Function_card_instruction_sheet.pdf
58	pdf	http://www.delta-electronics.info/content/files/DTV_manual_rus.pdf
59	pdf	http://www.delta-electronics.info/content/files/VFDL_manual_rus.pdf
60	pdf	http://www.delta-electronics.info/content/files/RTU_485_manual_rus.pdf
61	pdf	http://www.delta-electronics.info/content/files/Installation_Note_480W1PH_rus.pdf
62	pdf	http://www.delta-electronics.info/content/files/Installation_Note_60W3PH_rus.pdf
63	pdf	http://www.delta-electronics.info/userdata/files/Paketodelatel'naya_mashina.pdf
64	pdf	http://www.delta-electronics.info/content/files/Installation_Note_60W1PHplastic_rus.pdf
65	pdf	http://www.delta-electronics.info/content/files/DVP04AD_S_rus.pdf
66	pdf	http://www.delta-electronics.info/content/files/BUE_brake_unit_announcement.pdf

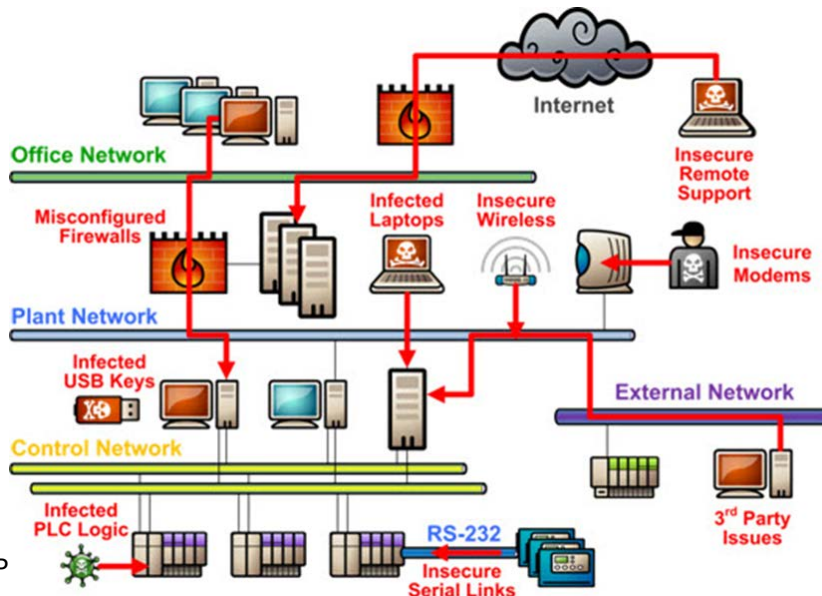
67	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
68	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
69	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
70	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
71	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
72	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
73	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
74	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
75	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
76	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
77	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
78	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
79	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
80	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
81	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
82	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
83	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
84	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
85	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
86	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
87	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
88	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
89	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
90	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
91	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
92	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
93	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
94	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
95	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
96	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
97	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf
98	pdf	http://www.delta-electronics.info/userdata/files/Kontrollery_certificate_PLCD_2013-2015.pdf
99	pdf	http://www.delta-electronics.info/userdata/files/Operat_paneli_certificate_HMI_2013-2015.pdf

112	pdf	http://www.delta-electronics.info/content/files/Sertifikat_servoprivody_Delta_Electronics.pdf
113	pdf	http://www.delta-electronics.info/userdata/files/Ustanovka_HI-Speed_VFD-B1.pdf
114	pdf	http://www.delta-electronics.info/content/files/VFD_Ext_cable.pdf
115	pdf	http://www.delta-electronics.info/content/files/Sertifika_temoregulatory_Delta_Electronics.pdf
116	pdf	http://www.delta-electronics.info/content/files/Sertifikat_HMI_Delta_Electronics.pdf
117	pdf	http://www.delta-electronics.info/userdata/files/DOP-A_v_proety_dlya_DOP-B.pdf
118	pdf	http://www.delta-electronics.info/userdata/files/Filtry_2012-2015.pdf
119	pdf	http://www.delta-electronics.info/content/files/Temperaturnyye_kontrollery_certificate_2012-2015.pdf
120	pdf	http://www.delta-electronics.info/userdata/files/Temperaturnyye_kontrollery_certificate_2012-2015.pdf
121	pdf	http://www.delta-electronics.info/content/files/Filtry_2012-2015.pdf
122	pdf	http://www.delta-electronics.info/userdata/files/Servodvigateli_certificate_2012-2015.pdf
123	pdf	http://www.delta-electronics.info/content/files/VFD_RC-01.pdf
124	pdf	http://www.delta-electronics.info/content/files/Servodvigateli_certificate_2012-2015.pdf



Sample Malware Analysis of Delta Elektronik (Delta Electronic) Online Files

DELTA_IA-PLC_DCISoft-V1.12_SW_20141211.zip **Trojan.DownLoader22.26498**
VFDSOFT 1.40 setup.zip **Backdoor/Sandrator.c** "Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP, Windows Vista, Windows 7 (x86/x64), Windows 8 (x86/x64), Windows 10 (x86/x64) - **virus.win32.virut.bn** - **Trojan.KillFiles.24350** - **virtool.win32.obfuscator.xy** - **Trojan.Generic-hlwMZB8tkIL (cloud)** - **virtool.win32.injector.bg!bit** - **Trojan.Win32.Agent"**
VFDSOFT 1.42 setup.zip **Backdoor/Sandrator.c**
VFD-VE_monitor_software.zip **Adware.OutBrowse.Win32.102234**
WPL2.11.60.zip **Backdoor/Sandrator.c**
DMT2.0.zip **Win32.Trojan.WisdomEyes.16070401.9500.9988**
PC-PLC_communication_libraries.rar **W32.Malware.Heur**
PC-PLC_communication_libraries.rar **Trojan.Kryptik.Win32.801938** backdoor / steals sensitive information:
searches for .doc .docx .eml files / searches for TellerPlus BanLine Fidelity



Files found on Deltaww.com site that goes out to all vendors. Pre-infected malware meaning their site is likely open to hack, files infiltrated, downloaded, infected, uploaded back to the Taiwanese site.



Yuri Chekunov

Director of public institutions "Tsentrospas-Yugoria"

Yuri Chekunov said:

- "The recognition of our achievements - is a definite indicator of a good job agencies in this area, because the work of firefighters and rescuers specifically associated with risk to life and is always traumatic. This is a huge incentive to continue to work in this direction at the highest level. Life and health of workers - the main goal and concern for the employer, it can not be measured by any awards. "
 - In "Tsentrospas-Yugoria" today, 9 branches, which cover 158 settlements. Public safety provides a staff of over 2500 people - it's fire departments, emergency rescue teams and civil defense units and emergency situations.

Director of public institutions of the Khanty-Mansiysk Autonomous Region –

Civil Protection Department of the Population of Khanty-Mansi Autonomous

District - Yugra

Yuri Chekunov

Owner of Spektr Elektro Servis and Centrospas-Yugoriya

Works for the government, has his own businesses, responds to Government RFPs, awards them to his own companies, sells SCADA Gear. Likely he pockets a cut and provides the Kremlin a cut. - Oligarch

KU "TCentrospas-YUgoriya" (kazennoe uchrezhdenie Hanti-Mansijskogo avtonomnogo regiona - YUgri "TCentrospas-YUgoriya". TIN: 8601025290, address: TYUMENSKAYA AREA.HANTI-MANSIJSKIJ AVT. OKRUG.G HANTI-MANSIJSK.UL POSADSKAYA, D 17)

filial KU "TCentrospas-YUgoriya" po Nizhneartovskomu (filial kazennogo uchrezhdeniya Hanti-Mansijskogo avtonomnogo regiona - YUgri "TCentrospas-YUgoriya" po Nizhneartovskomu rajonu, TIN: 8601025290, address: TYUMENSKAYA AREA.HANTI-MANSIJSKIJ AVT. OKRUG.NIZHNEARTOVSKIJ REGION.RP IZLUCHINSK.UL KEDROVAYA, D 5)

filial kazennogo uchrezhdeniya "TCentrospas-YUgoriya" po (filial kazennogo uchrezhdeniya Hanti-Mansijskogo avtonomnogo regiona - YUgri "TCentrospas-YUgoriya" po Nefteyuganskomu rajonu, TIN: 8601025290, address: 628331, Tyumenskaya area Nefteyuganskij rajon, rp Pojkovskij, promzona, d 16a)

filial kazennogo "TCentrospas - YUgoriya" po Berezovs (filial kazennogo uchrezhdeniya Hanti-Mansijskogo avtonomnogo regiona - YUgri "TCentrospas-YUgoriya" po Berezovskomu rajonu, TIN: 8601025290, address: 628140, Tyumenskaya area, Berezovskij rajon, rp Berezovo, ul Lyutova, d 13a)

filial KU HMAO- YU "TCentrospas-YUgoriya" po Beloyarskomu rajonu (filial Kazennogo uchrezhdeniya Hanti-Mansijskogo avtonomnogo regiona - YUgri "TCentrospas-YUgoriya" po Beloyarskomu rajonu, TIN: 8601025290, address: G TYUMEN,UL PERMYAKOVA, D 43A KAB 410)

filial "TCentrospas-YUgoriya" po Oktyabrskomu rajonu (filial kazennogo uchrezhdeniya Hanti-Mansijskogo avtonomnogo regiona-YUgri "TCentrospas-yugoriya" po Oktyabrskomu rajonu, TIN: 8601025290, address: 628126, Tyumenskaya area, Oktyabrskij rajon, rp Priobe, ul YUgorskaya, d 5)



BlackEnergy

Identified several years ago, BlackEnergy is a Trojan malware designed to launch distributed denial-of-service (DDoS) attacks, download custom spam, and banking information-stealer plugins.



- BlackEnergy malware was known to have been used to deliver KillDisk, a feature that could render systems unusable and could obliterate critical components on an infected system.
- It was reported to have possessed remarkable functions that could place Industrial Control Systems (ICS) at risk.
- An attack scenario involves a target receiving an email that contains a malicious attachment.
- The attacker spoofs the sender address in order to appear to be coming from Rada (the Ukrainian parliament).
- Once the target opens the attachment, the victim is asked to run the macro in the document.

2007 1st version of BlackEnergy appeared in 2007 DDoS attacks, create botnets, steal banking credentials

2008 - Russian-Georgian conflict, BlackEnergy used to conduct cyber-attacks against Georgia.

2009 - In Citibank attack, the attacker had stolen tens of millions of dollars.

2010 - BlackEnergy2 is released in 2010 supporting more plug-in features.

2014 - BlackEnergy defined Ukraine and Poland as its attack targets.

April-May 2007 Estonia angers Moscow planning move of Russian WWII memorial

June 2008 Lithuanian government outlaws display of Soviet symbols

August 2008 Georgia sends troops into breakaway republic backed by Moscow

January 2009 Persuading president of Kyrgyzstan to evict American military base

April 2009 Kazakhstan media publishes statement by their president criticizing Russia

2014 Pentagon blames Russia hack into White House's email with State Dept

March 2014 Russian-armed (little green men) pro-Russian rebels Russian Spetsnaz seize control of Crimea

May 2014 3-days prior to Ukraine's pres. election, Russian proxy groups take down election commission

October 2014 BlackEnergy attacks GE, Advantech WebAccess, SiemensWinCC.

October 14, 2014 BlackEnergy sample which is delivered via CVE-2014-4114.

November 2014 - Attack the devices of Linux and Cisco.

December 2014 Cyber-attack against the infrastructure of Germany

November 2015 - Election in Ukraine, KillDisk infected several media agencies.

December 2015 BlackEnergy should be responsible for energy blackouts

April 2015 Russia sought to destroy France's TV5Monde channel via cyberattack

May 2015: Germany discovered hackers penetrated computer network of German Bundestag

May 2015 Hackers tried to penetrate the computers of Chancellor Angela Merkel party

October 2015 NATO meeting in Bulgaria, websites of the council of ministers of Parliament and the central election committee were attacked

November 2015 Increased Russian incursions into their Bulgarian airspace

November 2015 Turkey shoots down Russian plane in its airspace

December 2015: Russian attack on Turkey forces closing of web traffic to .tr addresses

July-Dec 2016: 16 US Intel Agencies say Russian hacks Dems emails



Analysis of Delta Elektronics and BlackEnergy

We believe with moderate confidence that Delta Elektronics (DE) is likely a front company, and the equipment purchased from DE is vulnerable to supply chain threats. The possible supply chain threats introduce vulnerabilities impacting organizational supply chain functions and daily operations.

Evidence 1 (E1)	Evidence 2 (E2)	Evidence 3 (E3)	Evidence 4 (E4)	Evidence 5 (E5)	Evidence 6 (E6)
Embedded Malware	Oleg Strekozov – Fake Malware in Delta online software – docs – DeltaTW unaware	Oleg aligned with malware –Strekozov Dragonfly	Matrix Group LLC Chekunov – Oligarch Integrated with Gov Institutions	BlackEnergy progress, Maturity, targeting, Intent, speed, automation, motivation	Russian cyber Capabilities – org Structure – geo political tied to cyber

We believe with moderate confidence that Delta Elektronics (DE) and BlackEnergy are part of an integrated, hybrid warfare effort targeting actual and perceived threats to the Russian Federation. It is likely the behaviors exhibited are part of strategic positioning, maturation of the program, and demonstrated success of Russian cyber maskirovka and dezinformatsiya.





Final Analysis

Although there is an absence of evidence supporting a direct alignment of BlackEnergy, Dragonfly, and Delta Elektronik, the similarity of the targets, assumed adversary intent, the behaviors and methods of deception are consistent with nation-state actions.



We estimate the likelihood of Russian complicity to be probable. The evidence collected and subsequent analysis using structured techniques *does not render our judgment to be fact or a certainty, however, and such judgments still carry a risk of being wrong.*

Some of the information is fragmented and poorly corroborated to make solid analytic inferences. Some sources are difficult to validate. Typical compartmentalization of intelligence activities may be used to ensure complete lack of awareness of activities at the operational level. Leadership over the groups behind BlackEnergy, Dragonfly, and Delta Elektronik may be limited in a “*Dunbar’s number*” method of maintain secrecy.



Final Analysis

Although there is an absence of evidence supporting a direct alignment of BlackEnergy, Dragonfly, and Delta Elektronik, the similarity of the targets, assumed adversary intent, the behaviors and methods of deception are consistent with nation-state actions.



We estimate the likelihood of Russian complicity to be probable. The evidence collected and subsequent analysis using structured techniques *does not render our judgment to be fact or a certainty, however, and such judgments still carry a risk of being wrong.*

Some of the information is fragmented and poorly corroborated to make solid analytic inferences. Some sources are difficult to validate. Typical compartmentalization of intelligence activities may be used to ensure complete lack of awareness of activities at the operational level. Leadership over the groups behind BlackEnergy, Dragonfly, and Delta Elektronik may be limited in a “*Dunbar’s number*” method of maintain secrecy.



Intelligence Games in the Power Grid

Deception-Denial-Manipulation
Jeff Bardin – Treadstone 71
jbardin@treadstone71.com