

Intelligence Games in the Power Grid

Treadstone 71

originally created 2016

Contents

Intelligence Games in the Power Grid	1
Analytic Review	4
Delta Electronics highly likely supported by the Russian government and a direct threat to energy sector supply chain operations	4
Narrative Overview – Supporting Information	6
Chronology of Russian Attacks.....	7
BlackEnergy	9
Step 1: Reconnaissance and Intelligence Gathering	9
Step 2: Malware Development and Weaponization.....	10
Step 3: Deliver Remote Access Trojan (RAT).....	10
Step 4: Adversaries install BlackEnergy 3.....	10
Step 5: Establish CC Connection.....	11
Step 6: Deliver Malware Plugins	11
Step 7: Harvest Credentials.....	11
Step 8: Lateral Movement and Target Identification on Corporate Network	12
Step 9: Lateral Movement and Target Identification on ICS network	12
Step 10: Develop Malicious Computer Code	13
Step 11: Deliver Data Destruction Malware	13
Step 12: Schedule Uninterruptable Power Supply (UPS) Disruption	13
Step 13: Trip Breakers	14
Step 14: Sever Connection to Field Devices.....	14
Step 15: Telephony Denial-of-Service Attack.....	14
Step 16: Disable Critical Systems via UPS Outage.....	15
Step 17: Destroy Critical System Data.....	15
DragonFly	16
Background	16
Tools employed.....	17
Multiple attack vectors	17
Trojanized software	18
Delta Electronics	19
Intelligence/Reconnaissance:	19
OGRN.....	19
Delta Electronics and Dragonfly?.....	20
Raw data and information review	20
Gaps and Assumptions.....	22

Analysis of Competing Hypotheses I	25
Analysis of Competing Hypotheses II	26
In Summary	28
Bibliography	29

Analytic Review

Delta Elektronics highly likely supported by the Russian government and a direct threat to energy sector supply chain operations

The team asserts with moderate confidence that Delta Elektronics (DE) is likely a front company directly associated with Energetic Bear (Dragonfly), and the equipment purchased from DE is vulnerable to supply chain threats due to malware embedded in the Taiwanese Delta Electronics (T-DE) programmable logic controller (PLC) software (unbeknownst to T-DE). T-DE is not aware of the infections allowing customers to download and install infected PLC software for the initial purposes of cyber espionage. Long term intentions include possible physical sabotage operations. The PLCs appear to be genuine production parts with malware introduced post production. Verification of Oleg Vladimirovich Strekozov's identity is incomplete; the name is likely fictitious and probably state-sponsored. Evidence that suggests this

outcome:

Malware Targets SCADA Devices

- TTPs are like Dragonfly or Energetic Bear (B2)
- Targeting SCADA devices is consistent with espionage practices (B2)
 - Provides hackers a foothold into US critical infrastructure

Delta Website in Taiwan

- A copycat website in Russia is suspicious and consistent with masquerade techniques (C3)
- A legitimate Russian business would not conduct themselves in such a way (C2)
- Delta Electronics, based out of Taiwan and has no records of any locations in St. Petersburg (B2)

Many Russian Domains with Delta Names

- A legitimate business would not want to have such a disorganized web presence (C2)
 - 20+ companies founded under this name cover various market sectors and verticals (B2)
- Some of the websites are known to host a variety of malware (B2)
 - Multiple IP's registered by Oleg and flagged as malicious (B2)
- A registration certificate exists on delta-electronics.info supporting possible state-sponsorship (C3)

Other Information

- A bill of lading with the name "Oleg Vladimirovich Strekozov" (F3)
 - Strekozov coincidentally translates 'Dragonfly' as used by Symantec in early malware discoveries (B2)
- Physical locations for DE appear to be vacant lots, apartment buildings, and non-SCADA businesses (C3)
 - Matrix Group LLC (DE owner) physical location secured with gates, fences, keypad access devices, and security cameras (C2)
 - The Matrix Group LLC lists over 260 domain names of varying legitimacy (B2)
 - The location of NPO Stoik, a business named in document metadata found on Delta Elektronics websites, is in Moscow, and, along with several other associated addresses and likely near buildings used by Russian intelligence agencies (F3)

Reliability of Source		Credibility of the Information	
A	Completely reliable	1	Confirmed by other sources
B	Usually reliable	2	Probably true
C	Fairly reliable	3	Possibly true
D	Not usually reliable	4	Doubtful
E	Unreliable	5	Improbable
F	Reliability cannot be judged	6	Truth cannot be judged



Yuri Chekunov

Director of public institutions "Tsentropas-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 "Tsentropas-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 Spektro 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 "Tsentropas-Yugoria" является учреждением Ханты-Мансийского автономного округа - Югры "Тентропас-Югория". TIN: 44012296, адрес: ТУМЕНСКАЯ ОБЛАСТЬ/МАНСЕЙСКИЙ ОУГ/ОБЩЕСТВЕННАЯ АДМИНИСТРАЦИЯ ПОДРАЗДЕЛЕНИЯ Д.17

филиал КУ "Тентропас-Югория" по Нижнеуральскому округу филиал кантонного учреждения Ханты-Мансийского автономного округа - Югры "Тентропас-Югория" по Нижнеуральскому району. TIN: 44012296, адрес: ТУМЕНСКАЯ ОБЛАСТЬ/МАНСЕЙСКИЙ ОУГ/ОБЩЕСТВЕННАЯ АДМИНИСТРАЦИЯ ПОДРАЗДЕЛЕНИЯ Д.17

филиал кантонного учреждения "Тентропас-Югория" по Югорийскому району филиал кантонного учреждения Ханты-Мансийского автономного округа - Югры "Тентропас-Югория" по Югорийскому району. TIN: 44012296, адрес: 620111, Тюменская обл. Югорийский район, ул.Победы, д.10а

филиал кантонного "Тентропас - Югория" по Везовскому отделу кантонного учреждения Ханты-Мансийского автономного округа - Югры "Тентропас-Югория" по Везовскому району. TIN: 44012296, адрес: 62149 Тюменский обл. Везовский район, ул.Возврата, д.14а

филиал КУ ИМАО- ЮГ "Тентропас-Югория" по Белоярскому району отдел кантонного учреждения Ханты-Мансийского автономного округа - Югры "Тентропас-Югория" по Белоярскому району. TIN: 44012296, адрес: 61 ТУМЕНСКАЯ ОБЛАСТЬ/ЮГОРИЯ, Д.41 КАМ.410

филиал "Тентропас-Югория" по Октябрьскому району отдел кантонного учреждения Ханты-Мансийского автономного округа - Югры "Тентропас-Югория" по Октябрьскому району. TIN: 44012296, адрес: 620111, Тюменская обл. Октябрьский район, ул.Победы, д.17 Югория, д.17



Readstone 71

- Yuri Chekunov, Director at a government organization in Khanti-Mansi district owns firms that buy and sell SCADA equipment (C3)
 - Yuri's firms have direct relationships with DE (B2)
 - Mr. Chekunov approves contracts for the government that his company's bid on (F3)
 - It is likely that Mr. Chekunov is part of the Russian oligarchy (F3)

The team recommends placing a company service call to evaluate if anyone tampered with the suspected hardware. Team 1 recommends reducing production levels to minimize safety issues or equipment damage. Manual inspection of purchased DE equipment required.

We recommend the following:

- A complete scan, reverse engineering, and analysis of the software provided in a sandbox environment
- Identification of other SCADA companies providing downloadable PLC software
 - Review and analysis of this software
- Engagement with T-DE to determine extent of the infections
 - Examine web logs to determine downloads by clients
 - Incident declaration and full examination of external hacking and insider threats
- Engagement with authorities to identify possible US infections and exploitation

Intelligence gaps include:

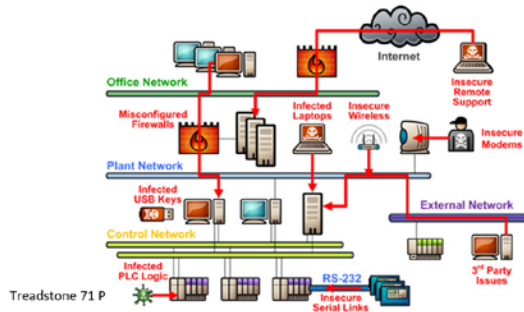
- Whether other malware campaigns intersect with this activity
- Whether any Chinese organization or agency stands to financially gain from this activity
- If any data has been exfiltrated due to the malware
- The scope of malware infections at other SCADA companies
- Tangible evidence tying DE to the malware on T-DE websites

Alternative Analysis

We assess with low confidence that Delta Elektronics is a third-party organization sponsored by the Russian government or is a false flag operations posing as a supplier to legitimate electronic company hardware inserting malware into foreign industrial supply chains for espionage purposes. An equally plausible assessment (low confidence) is that DE is a front company used by criminals to either sell counterfeit equipment or to conduct a fraudulent "middle man" operation to take a cut of the profit from the sale of legitimate equipment.

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-hlwMZB8tkL (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 BancLine 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.

Narrative Overview – Supporting Information

The behavior analysis topic will be used to discuss a combined case studies related to SCADA systems and the sale of SCADA hardware and associated software that could be spiked (loaded with malware). The case study would focus on potential Russian activities in this area, their creation of fake companies, their duplication of websites and website content to make them look legitimate, and the tracking of the potential people behind this to other malicious cyber activities.

“A new type of war has emerged, in which armed warfare has given up its decisive place in the achievement of the military and political objectives of war to another kind of warfare - information warfare.”

Infiltrating systems in the deployment phase is attractive as this does not require the devices themselves to be vulnerable. As SCADA systems generally are very poorly maintained, with patch penetrations bordering towards 0% when we have been able to observe penetration on the market. The intentions apart from directly affecting those systems as means in a conflict, they are often deployed on networks from where they can reach other internal resources. Being able to infect devices which are likely to spend 10 to 20 years on a network largely unmaintained is one of the most stable sources of persistence a threat actor can obtain. This means the devices not only provide means of controlling critical infrastructure in other nations, but it is also a means of obtaining access to other internal resources for an extended period.

Take for example the BlackEnergy attacks against Ukrainian SCADA assets. Assumed Russian cyber adversaries disrupted power grid operations causing blackouts for over 225,000 customers in Ukraine. The attack was highly complex using a methodical approach to planning, direction, intelligence collection, resource utilization, mission management, expert skills, highly malicious payloads, and combinations of manual, semi, continuous levels of automation.

Targeted intellection collection started months before the attack execution. Run like a well-managed special forces operation, the adversaries clandestinely created persistent access footholds to multiple industrial networks, identified Ukrainian energy-related targets, before carrying out an integrated, complex, and process-driven operation that disrupted electricity distribution and destroyed various systems, flooded call centers, distorted internal systems, and impeded incident response. Based upon system design and intelligence on the target, malware deployed by the adversaries exploited weaknesses in access protocols to gain administrative access to critical systems. Once inside, adversaries created valid administrative accounts enabling lateral movement across trusted systems. The adversaries achieved their goals by shutting down power distribution to key functions of the grid.

Another possible aspect of exploiting SCADA systems starts at the physical level. Russian corporations are mimicking global organizations that research and development, design, manufacture, and sale of electronic control systems, industrial automation products, digital display products, communication products, consumer electronics products, energy-saving lighting application, and energy technology (DLELY Key Statistics - Delta Electronics Inc., 2017) services. One such organization is Delta Electronics from Taiwan.

The accelerating trends of supply chain globalization and outsourced manufacturing and distribution have combined to increase the pace of change, complexity, and risk for brand owners. These trends have created a fundamental shift in the way companies of all sizes plan, source, make, and deliver their goods and services. The Russian focus to actively target various phases of the supply chain makes for malware installation to be viewed as normal network activity. An activity that is deemed normal upon installation of the hardware and software in question.

Supply chains are difficult to secure; they create a risk that is hard to identify, complicated to quantify and costly to address. A compromise anywhere in the supply chain can have just as much impact on your organization, and its reputation, as one from within the organization. There is great necessity to track everything that is happening in the supply chain as even the smallest supplier, or the slightest hiccup can have a dangerous impact on your business.

The cyber security industry has already seen USB-devices shipped with malware straight out of the factory, just as we have seen CD's from magazines with malware during the 90's. Affecting devices in the production line is of course equally tempting to actors from Russia as it is for the NSA. A state actor focusing on monitoring citizens has different requirements

from a nation building its cyber arms arsenal. Where the NSA had a focus on networking equipment and traffic monitoring, this makes the same degree of sense from a cyber arms perspective.

Russian methods of information influence and information operations include network operations alongside disciplines such as psychological operations, strategic communications, Influence, along with “intelligence, counterintelligence, maskirovka, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, and destruction of enemy computer capabilities. Taken together, this forms a whole of systems, methods, and tasks to influence the perception and behavior of the enemy, population, and international community on all levels.

One fundamental distinction between Russian and Western approaches to information activities is the categorization of computer network operations and other activities in cyberspace.

“Cyber” as a separate function or domain is not a Russian concept. The delineation of activities in the cyber domain from other activities processing, attacking, disrupting or stealing information is seen as artificial in Russian thinking. In this context, “Distributed denial of services attacks (DDoS), advanced [cyber] exploitation techniques and Russia Today television are all related tools of information warfare.

A key concept often lost on the West is Russia’s willingness to give primacy to non-kinetic operations, especially information warfare. The Western assumption has been that subversion, deception, and the like are all ‘force multipliers’ to the combat arms, not forces in their own right. At present, though, Russia is clearly seeing the kinetic and the non-kinetic as interchangeable and mutually supporting.

Russia's use of the tools of information pressure - a key theme of the latest statements by the representatives of the state administration sector in Ukraine. At the same time, Russia denies any involvement in the facts of information aggression: hacking databases, network services and the use of information technology for propaganda purposes.

The Russian targeting of various phases of the SCADA supply chain represents information-technology warfare (to affect technical systems which receive, collect, process and transmit information), which is conducted during wars and armed conflicts. The behaviors exhibited by the perpetrators is not usually targeted. Examining Russian activities within the SCADA supply chain requires analysis focused on users, user accounts, user identities, and the sources of their activities.

Openly selling to various Western, Asian, and Middle Eastern energy organizations who purchase from these known companies is a method to infiltrate critical infrastructures in target organizations globally. The potential for use later is part of an overall sea, air, land, cyber integrated strategy of hybrid warfare.

This is but one aspect of hybrid warfare attacks against the energy sector. The use of malicious code such as BlackEnergy serves as a reminder of the combined efforts by adversaries in using access to hardware in the supply chain and external infiltration of this hardware without attribution. Since the December 2015 attack against Ukraine’s power grid, the Ukraine has experienced 6,500 cyber hacks to state institutions in November and December 2016 alone. Ukraine has accused Russia of these cyber-attacks, but Moscow has denied involvement. A standard behavior of non-attributable, hybrid warfare. (Douris, 2017)

Chronology of Russian Attacks (Timeline: Ten Years of Russian Cyber Attacks on Other, n.d.)

Russian cyber attacks normally occur in conjunction with geopolitical events. They are part of his overall scheme of hybrid warfare. Amid a show of hybrid tactics, Putin has awarded financial support to fringe political movements in Western Europe, launched cyberattacks and espionage in Europe, and ordered probing and actual attacks on U.S. and European energy and communications infrastructure. He has continued to attempt to use control over energy – pipelines, nuclear plants, natural gas supplies – to wield influence across Europe. Western intelligence reports say Russia has exacerbated the Syrian migrant crisis. And, compounding the threat, Russia has formed a growing alliance with Iran and China, countries

that possess their own hybrid toolboxes of proxy warfare and cyber infiltration. (Mazarr, 2015) Another standard behavior of hybrid warfare and one used against the energy sector.

Russia's actions based upon 'maskirovka' deploys few military assets while coordinating multiple functions of disinformation, psychological warfare, memetic engineering, and deception to achieve goals. Russia's actions are likened to placing a frog in a pot of cool water on a stove. While slowly heating up the water, the frog finds it difficult to notice the increasing temperatures until it is too late. All the time not knowing who actually placed him (the frog) in the water and not knowing who continued to turn up the burner. Maskirovka translates to camouflage but is also defined as the elements of surprise, diversion, and deception. Russia's asymmetrical activity prevails on the internet, in social media, and as truth and is inclusive of all functions of warfare. The methods are relatively cheap and capitalize on the years of studying Western behaviors. Russia is able to hack, infiltrate, manipulate, and manage the perceptions of targets while ensuring plausible deniability. They do so by using proxy groups, hackers for hire, and trained operatives all behind a monitor and keyboard.

- April - May 2007: Estonia, a tiny Baltic nation that was occupied by the Soviet Union until 1991, angered Moscow by planning to move a Russian World War II memorial and Russian soldiers' graves. Russia retaliated by temporarily disabling Estonia's internet, an especially harsh blow to the world's most internet-dependent economy. The distributed denial of service (DDoS) attack focused on government offices and financial institutions, disrupting communications.
- June 2008: In a similar attack, Russia punished another former possession in the Baltic. When the Lithuanian government outlawed the display of Soviet symbols, Russian hackers defaced government web pages with hammer-and-sickles and five-pointed stars.
- August 2008: After Georgia's pro-Western government sent troops into a breakaway republic backed by Moscow, Russian land, sea and air units invaded the country - and Russian hackers attacked Georgia's internet, the first-time Russia coordinated military, and cyber action. Georgia's internal communications were effectively shut down.
- January 2009: As part of an effort to persuade the president of Kyrgyzstan to evict an American military base, Russian hackers shut down two of the country's four internet service providers with a DDOS attack. It worked. Kyrgyzstan removed the military base. Subsequently, Kyrgyzstan received \$2 billion in aid and loans from the Kremlin.
- April 2009: After a media outlet in Kazakhstan published a statement by Kazakhstan's president that criticized Russia, a DDOS attack attributed to Russian elements shut down the outlet.
- August 2009: Russian hackers shut down Twitter and Facebook in Georgia to commemorate the first anniversary of the Russian invasion.
- 2014 – The Pentagon blamed Russia for a sophisticated hack into the White House's unclassified email correspondence and the State Department.
- March 2014: For the second time, the Russian government allegedly coordinated military and cyber action. A DDOS attack 32 times larger than the largest known attack used during Russia's invasion of Georgia disrupted the internet in Ukraine while Russian-armed pro-Russian rebels were seizing control of the Crimea. (JohnIB, n.d.)
- May 2014: Three days before Ukraine's presidential election, a Russia-based hacking group, took down the country's election commission in an overnight attack. Even a back-up system was taken down, but Ukrainian computer experts were able to restore the system before election day. Ukrainian police say they arrested hackers who were trying to rig the results. The attack was aimed at creating chaos and hurting the nationalist candidate while helping the pro-Russian candidate. Russia's preferred candidate lost.
 - BlackEnergy Chronology
 - 2007 - The first version of BlackEnergy appeared in 2007 used to launch DDOS attacks, create botnets and steal banking credentials and so on. (Antiy, n.d.)

- 2008 - During the 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 - The updated version BlackEnergy defined Ukraine and Poland as its attack targets.
 - October 2014 - BlackEnergy attacks HMI of several providers, the victims include GE, Advantech WebAccess, SiemensWinCC.
 - 14 October 2014 - iSIGHT discovered BlackEnergy sample which is delivered via CVE-2014-4114.
 - November 2014 - Attack the devices of Linux and Cisco.
 - December 2014 - The Information Security Report published German Federal Office for Information Security (BSI) in 2014 a cyber-attack against the infrastructure of one German mill. The attack caused significant physical damage. Reports indicated that the incident was related to BlackEnergy.
 - November 2015 - During the presidential election in Ukraine, KillDisk infected several media agencies.
 - December 2015 - Ukraine government asserted that BlackEnergy should responsible for the blackout incidents in the region of Lavno-Franklvst of Ukraine.
- May 2015: German investigators discovered hackers had penetrated the computer network of the German Bundestag, the most significant hack in German history. The Bundesamt für Verfassungsschutz (BfV), German's domestic intelligence service, later said Russia was behind the attack and that they were seeking information not just on the workings of the Bundestag, but German leaders and NATO, among others. Security experts said hackers were trying to penetrate the computers of Chancellor Angela Merkel's Christian Democratic party.
 - 2015 – France Russia sought to destroy France's TV5Monde channel via an April 2015 cyberattack. The attack took the channel off air for several hours.
 - October 2015 - At the November NATO meeting in Bulgaria, its prime minister explained that Starting on 25 October, websites of the council of ministers of Parliament and the central election committee were attacked through cyber capabilities in an unprecedented way. The Prime Minister blamed the Russians for the attacks, as it also coincided with increased incursions into their airspace by Russian planes.
 - 2015: Turkey blamed Russia for a massive cyber-attack that forced it to close external traffic to NIC.tr, making it impossible to access or send email from .tr addresses. Turkey had been at odds with Russia after shooting down a Russian plane in its airspace.
 - 2016: US Democratic National Committee. Starting with the Democratic National Convention and continuing into the fall campaign, Julian Assange's WikiLeaks has released emails purportedly coming from the Democratic National Committee and the Clinton campaign. A Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence put the blame squarely on the Russians.

BlackEnergy

Execution and Behavior

Step 1: Reconnaissance and Intelligence Gathering. Before the attack, adversaries likely begin open-source intelligence gathering and reconnaissance on potential targets. (WHEN THE LIGHTS WENT OUT, n.d.)

Location: External infrastructure Action: Active threat actor activity Timeline: May 2014 or earlier

Device/application: Activity conducted external to network

Role in infrastructure: Activity conducted external to network

Exploitation method: Adversaries likely gather publicly available information on deployed systems and network architecture, and may also use active discovery methods such as scanning of perimeter devices, enumeration of devices, social media data collection and analysis for future targeting

Step 2: Malware Development and Weaponization. Adversaries acquire or independently develop the malware to be used in the attack, as well as the weaponized documents to deliver malware.

Location: External infrastructure Action: Active threat actor activity Timeline: May 2014 or earlier

Device/application: Activity conducted external to network

Role in infrastructure: Activity conducted external to network

Exploitation method: Adversaries acquire BlackEnergy remote access Trojan (RAT) and weaponize Microsoft (MS) Word and Excel files with VBA scripts to drop the BlackEnergy RAT.

Impact: Combined with targeting data gathered during the reconnaissance phase, adversaries can develop tailored attack packages. At the completion of this step, adversaries have the necessary tools to begin their attack.

Step 3: Deliver Remote Access Trojan (RAT) Adversaries initiate phishing campaign against electricity distributors. **Step 4: Install RAT.** Adversaries install BlackEnergy 3 on each of the three targeted electricity distributors after employees open the weaponized MS Office email attachments and enable macros.

Location: Corporate network Action: Active threat actor activity Timeline: May 2014–June 2015e

Device/application: Employee workstations, likely using MS Windows OS and provisioned with MS Internet Explorer web browser

Role in infrastructure: Support email communications and other IT services used in business operations.

Exploitation method: Adversaries send targeted emails containing the modified MS Office files as attachments to users on targeted networks.

Impact: RAT is delivered to targeted network, but not installed. Installation requires employees to actively grant permission to the embedded VBA scripts to execute.

Step 4: Adversaries install BlackEnergy 3 on each of the three targeted electricity distributors after employees open the weaponized MS Office email attachments and enable macros.

Location: Corporate network

Action: Employee-enabled malware execution

Timeline: May 2014–June 2015

Device/application: Employee workstations, likely using MS Windows OS and provisioned with MS Internet Explorer web browser

Role in infrastructure: Support email communications and other services used in business operations.

Exploitation method: In a social engineering attack, employees are prompted to enable macros when opening the file attached to phishing email. Once macros are enabled, the VBA script places multiple malicious files on the workstation, unbeknown to the employee.

Impact: Files placed on workstations within the corporate network can begin the communication process with external Command and Control (CC) servers.

Step 5: Establish CC Connection. Malware establishes connection from the malicious implant on the targeted network to attacker-controlled CC server.

Location: Corporate network Action: Malware execution Timeline: May 2014–June 2015

Device/application: Employee workstations, likely using MS Windows OS and provisioned with MS Internet Explorer web browser

Role in infrastructure: Support email communications and other services used in business operations.

Exploitation method: The external connection is established as part of the execution routine following installation of the malicious files. Once permissions to execute macros are granted by employees, the malicious VBA script installs the malware implant, and the implant attempts to communicate with an external server via HTTP requests.

Impact: Adversaries gain unauthorized access to targeted networks, including the ability to deliver additional BlackEnergy plugins to enable internal network reconnaissance and credential harvesting.

Step 6: Deliver Malware Plugins Following installation of BlackEnergy 3 implant, adversaries likely import plugins to enable credential harvesting and internal network reconnaissance.

Location: Corporate network

Action: Active threat actor activity Timeline: June 2015–December 2015 Device/application: Employee workstations,

likely using MS Windows OS and provisioned with MS Internet Explorer web browser

Role in infrastructure: Support email communications and other services used in business operations

Exploitation method: The BlackEnergy 3 implant delivered in the initial attack functions as a receiver for additional malware plugins. After establishing a remote connection with delivered files via HTTPS, the threat likely delivers the additional malware components.

Impact: The delivered plugins enable additional BlackEnergy functionality, including harvesting user credentials, keylogging, and network reconnaissance.

Step 7: Harvest Credentials. Delivered BE3 malware plugins conduct credential harvesting and network discovery functions.

Delivered BlackEnergy 3 malware plugins conduct credential harvesting and network discovery functions.

Location: Corporate network

Action: Active threat actor activity, malware execution

Timeline: June 2015–December 2015

Device/application: Windows OS workstations, Windows domain controllers, virtual private network (VPN) service deployed in control environment

Role in infrastructure: These systems support business operations, manage permissions and domain access, and provide remote network access respectively.

Exploitation method: Adversaries use delivered BlackEnergy 3 plugins to gather stored credentials or log keystrokes. After gathering valid credentials for user with administrator privileges, adversaries use the stolen

administrator credentials to access the domain controller, recover additional credentials, and create new privileged accounts.

Impact: Adversaries obtain valid credentials enabling them to expand access across the corporate network and into the control environment, ensure persistent access, and blend into regular network traffic.

Step 8: Lateral Movement and Target Identification on Corporate Network

Adversaries conduct internal reconnaissance on corporate network to discover potential targets and expand accessed.

Location: Corporate network

Action: Active threat actor activity, malware execution Timeline: June 2015–December 2015

Device/application: Discovered systems, including networked uninterruptible power supply (UPS) devices, data center servers, a telephone communications server, and employee workstations

Role in infrastructure: Internal reconnaissance efforts could potentially include all deployed devices on the corporate network.

Exploitation method: Adversaries likely use a combination of valid user credentials and BlackEnergy 3 plugins developed to conduct network discovery. VS.dll plugin is likely used to leverage MS Sysinternals PsExec to establish remote connections to workstations and servers.

Impact: Adversaries can enumerate the systems deployed across the network, identify targets, and begin preparations for final attack.

Step 9: Lateral Movement and Target Identification on ICS network

Adversaries use stolen credentials to access the control environment and conduct reconnaissance on deployed systems.

Location: ICS network

Action: Active threat actor activity

Timeline: June 2015–December 2015

Device/application: Discovered systems, including human machine interface (HMI) workstations, distributed management system (DMS) servers, UPS devices, 52 serial-to-Ethernet converters (Moxa UC 7408-LX-Plus, 53 IRZRUH2 3G54), remote terminal unit (RTU) devices (ABB RTU560 CMU-02), and the substation breakers

Role in infrastructure: HMI workstations provide a graphical user interface for operators to remotely monitor and control devices within the control environment.

DMS applications enable centralized monitoring and issuing of commands within a control environment. UPS devices condition incoming power to downstream devices and provide temporary battery backup power. Serial-to-Ethernet converters convert serial data from field devices to digital packets, enabling communications with the control center. RTU devices function as a communication processor or a data concentrator in a substation, enabling communications and data transfer between field devices in the substations and the control center. Substation breakers are devices designed to physically interrupt current flows through an electrical circuit.

Exploitation method: Adversaries use valid credentials to interact directly with the client application for the DMS server via a VPN, and native remote access services to access employee workstations hosting HMI applications. This access likely enables adversaries to enumerate all networked devices within the control environment.

Impact: Adversaries gain access to critical systems, enabling them to begin target selection and preparations for final attack.

Step 10: Develop Malicious Computer Code. Adversaries develop malicious computer code update for identified serial-to-Ethernet converters.

Location: External infrastructure Action: Active threat actor activity Timeline: June 2015–December 2015

Device/application: Activity conducted external to network

Role in infrastructure: Activity conducted external to network

Exploitation method: After identifying deployed converters, adversaries begin a malware development and testing effort on infrastructure outside of the targeted network.

Impact: Upon completion of this step, adversaries would have target-specific malware designed to disrupt communications with field devices by disabling deployed converters.

Step 11: Deliver Data Destruction Malware. Adversaries likely deliver KillDisk malware to a network share and set policy on the domain controller to retrieve malware and execute upon system reboot.

Location: Corporate and ICS network

Action: Active threat actor activity

Timeline: December 2015, directly preceding attack

Device/application: Network share and Windows domain controller server

Role in infrastructure: The network share provides access to shared digital resources, and the Windows domain controller manages access control throughout the network.

Exploitation method: Adversaries likely use stolen credentials to place KillDisk malware on a network share, then set the retrieval and execution of the malicious files by implementing a policy on the compromised domain controller server.

Impact: Prescheduling execution of malware enables coordination of multiple attack components, such that data destruction coincides with or shortly follows attacks against breakers.

Step 12: Schedule Uninterruptable Power Supply (UPS) Disruption. Adversaries schedule unauthorized outage of UPS for telephone communication server and data center servers.

Location: Corporate and ICS network

Action: Active threat actor activity

Timeline: Directly preceding December 2015 attack

Device/application: Networked UPS devices with remote management interface

Role in infrastructure: Prevent power outages from disrupting continuous operation of critical systems.

Exploitation method: Adversaries likely use valid credentials to access privileged employee accounts, then use this access to remotely schedule unauthorized power outages.

Impact: Prescheduling outages enables coordination of multiple attack components, such that critical systems also go down because of the power outages, stifling potential restoration efforts.

Step 13: Trip Breakers. Adversaries use native remote access services and valid credentials to open breakers and disrupt power distribution to over 225,000 customers within three distribution areas.

Location: ICS network

Action: Active threat actor activity

Timeline: December 23, 2015, during

Device/application: HMI workstations, DMS servers, RTU, and the substation breakers

Role in infrastructure: HMI workstations provide a graphical user interface for operators to remotely monitor and control devices within the control environment.

DMS applications enable centralized monitoring and issuing of commands within a control environment.

Substation breakers are devices designed to physically interrupt current flows through an electrical circuit.

Exploitation method: Adversaries use valid credentials to seize control of operator workstations, access DMS client application via VPN, and issue unauthorized commands to breakers at substations.

Impact: Opening of breakers results in disruption of electricity service to customers.

Step 14: Sever Connection to Field Devices. After opening the breakers, adversaries deliver malicious computer code update to serial-to-Ethernet communications devices. The malicious updates render the converters inoperable, and sever connections between the control center and the substations.

Location: ICS network

Action: Active threat actor activity

Timeline: December 23, 2015, during attack

Device/application: Serial-to-Ethernet converters (Moxa UC 7408-LX-Plus, 55 IRZRUH2 3G56)

Role in infrastructure: Convert serial data from field devices to digital packets to be transmitted to remote monitoring and administration systems within the control network.

Exploitation method: Adversaries use network access to push the malicious update over the network to targeted devices.

Impact: Operators are unable to remotely close the breakers, requiring workers to manually close breakers at each substation. Forcing this manual response draws out recovery time

Step 15: Telephony Denial-of-Service Attack. Adversaries initiate DoS attack on telephone call center at one of the targeted distributors.

Location: Corporate network

Action: Likely automated process

Timeline: Dec 23, 2015, during attack

Device/application: Operator telephone call center

Role in infrastructure: Receive external telephone communications from customers.

Exploitation method: Adversaries likely use automated IP-based call generators to flood the targeted call center.

Impact: Automated calls overwhelm resources at call center, blocking legitimate communications from customers.

Step 16: Disable Critical Systems via UPS Outage. Previously scheduled UPS outage cuts power to targeted telephone communications server and data center servers.

Location: Corporate and ICS network Action: Execution of prescheduled process Timeline: December 23, 2015, during attack

Device/application: Networked UPS devices with remote management interface, telephone communications server, and data center servers

Role in infrastructure: Prevent power outages from disrupting continuous operation of critical systems.

Exploitation method: Adversaries use network access to schedule the temporary backup power to be offline at the time of the power outages.

Impact: Power loss to telephone server disrupts communications across remote sites, and disruptions at control centers inhibit ability to monitor and respond to attack against breakers. The disruption at the data center and associated system reboot trigger execution of KillDisk malware.

Step 17: Destroy Critical System Data. Scheduled execution of KillDisk malware erases the master boot records and deletes system log data on targeted machines across the victims' corporate and ICS network.

Location: Corporate network and ICS network

Action: Malware execution

Timeline: December 23, 2015, during attack

Device/application: RTU device (ABB RTU560 CMU-02), 57 servers and workstations used by management, human resources (HR), and finance staff

Role in infrastructure: The RTU functions as a communication processor or data concentrator in a substation, enabling communications and data transfer between field devices in the substations and the control center. 58 Servers and workstations are used by management, HR, and finance staff to conduct business administration operations.

Exploitation method: Malware is retrieved from the network share and executed on networked devices according to direction received via domain controller policy or local Windows Task Scheduler.

Impact: Targeted systems are rendered inoperable, and critical data is destroyed.

DragonFly

An ongoing cyberespionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims. The attackers, known to Symantec as Dragonfly, managed to compromise (Star Report, n.d.) some strategically important organizations for spying purposes and, if they had used the sabotage capabilities open to them, could have caused damage or disruption to energy supplies in affected countries.

Among the targets of Dragonfly were energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers. The majority of the victims were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland. (Dragonfly, n.d.)

The Dragonfly group is well resourced, with a range of malware tools at its disposal and is capable of launching attacks through some different vectors. Its most ambitious attack campaign saw it compromise some industrial control system (ICS) equipment providers, infecting their software with a remote access-type Trojan. This caused companies to install the malware when downloading software updates for computers running ICS equipment. These infections not only gave the attackers a beachhead in the targeted organizations' networks but also gave them the means to mount sabotage operations against infected ICS computers.

This campaign follows in the footsteps of Stuxnet, which was the first known major malware campaign to target ICS systems. While Stuxnet was narrowly targeted at the Iranian nuclear program and had sabotage as its primary goal, Dragonfly appears to have a much broader focus with espionage and persistent access as its current objective with sabotage as an optional capability if required.

In addition to compromising ICS software, Dragonfly has used spam email campaigns and watering hole attacks to infect targeted organizations. The group has used two main malware tools: Backdoor.Oldrea and Trojan.Karagany. The former appears to be a custom piece of malware, either written by or for the attackers.

Before publication, Symantec notified affected victims and relevant national authorities, such as Computer Emergency Response Centers (CERTs) that handle and respond to Internet security incidents.

Background

The Dragonfly group, which is also known by other vendors as Energetic Bear, appears to have been in operation since at least 2011 and may have been active even longer than that. Dragonfly initially targeted defense and aviation companies in the US and Canada before shifting its focus mainly to US and European energy firms in early 2013.

The campaign against the European and American energy sector quickly expanded in scope. The group initially began sending malware in phishing emails to personnel in target firms. This behavior changed to watering hole attacks compromising websites likely to be visited by those working in energy to redirect them to websites hosting an exploit kit. The exploit kit, in turn, delivered malware to the victim's computer. The third phase of the campaign was the Trojanizing of legitimate software bundles belonging to three different ICS equipment manufacturers. These behaviors represent a combined approach that continues to evolve but ensures weaknesses in software and the supply chain are equally exploited.

Dragonfly's behavior is representative of a state-sponsored operation. Dragonfly mounts attacks through multiple vectors and compromise numerous third party websites in the process as a tool to ensure anonymity. Dragonfly targeted several organizations in the energy sector. Its current main motive appears to be cyberespionage, with sabotage a definite secondary capability potentially for later use.

Time analysis behaviors of timestamps on the malware used by the attackers indicates that the group mostly worked between Monday and Friday, with activity mainly concentrated in a nine-hour period that corresponded to a 9 am to 6 pm working day in the UTC +4 time zone. Based on this information, it is likely the attackers are based in Eastern Europe. (Energy Sector Alert, n.d.)

Tools employed

Dragonfly uses two main pieces of malware in its attacks. Both are remote access tool (RAT) type malware which (Dragonfly vs. America, Courtesy of Russia , n.d.) provides the attackers with access and control of compromised computers. Dragonfly's favored malware tool is Backdoor. Oldrea, which is also known as Havex or the Energetic Bear RAT. Oldrea acts as a backdoor (Symantec, n.d.; Symantec, n.d.) for the attackers on to the victim's computer, allowing them to extract data and install further malware.

Oldrea appears to be custom malware, either written by the group itself or created for it. This provides some indication of the capabilities and resources behind the Dragonfly group.

Oldrea's behavior once installed is to gather system information, along with lists of files, programs installed, and the root of available drives. It will also extract data from the computer's Outlook address book and VPN configuration files. This data is then written to a temporary file in an encrypted format before being sent to a remote command-and-control (C&C) server controlled by the attackers. The file obfuscation ensures anonymity of content.

The C&C servers appear to be hosted on compromised servers running content management systems, indicating that the attackers may have used the same exploit to gain control of each server. This behavior follows the model of maskirovka. Oldrea has a basic control panel which allows an authenticated user to download a compressed version of the stolen data for each particular victim.

The second main tool used by Dragonfly is Trojan.Karagany. Unlike Oldrea, Karagany was available on the underground market. The source code for version 1 of Karagany was leaked in 2010. Symantec believes that Dragonfly may have taken this source code and modified it for its own use thereby further validating the risk of leaving cyber weaponry on the battlefield. This version is detected by Symantec as Trojan.Karagany!gen1.

Karagany is capable of uploading stolen data, downloading new files, and running executable files on an infected computer. Karagany has additional behaviors such as running additional plugins, using tools for collecting passwords, taking screenshots, and cataloging documents on infected computers. The intent to analyze the data for later exploitation.

Symantec found that the majority of computers compromised by the attackers were infected with Oldrea. Karagany was only used in around 5 percent of infections.

Multiple attack vectors

The Dragonfly group has used at least three infection behaviors against targets in the energy sector. The initial behavior was an email campaign, which saw targeted executives and senior employees in energy companies receive emails containing a malicious PDF attachment. Infected emails had one of two subject lines: "The account" or "Settlement of delivery problem".

The spam campaign began in February 2013 and continued into June 2013. Symantec identified seven different organizations targeted in this campaign. This behavior ceased as organizational defenses improved.

The attackers then shifted their behaviors to watering hole attacks, comprising some energy-related websites and injecting an iframe into each which redirected visitors to another compromised legitimate website hosting the Lightsout exploit kit. Lightsout exploits either Java or Internet Explorer to drop Oldrea or Karagany on the victim's computer. The fact that the attackers compromised multiple legitimate websites for each stage of the operation is further evidence that the group has strong technical capabilities while changing tactics. The tactics may have changed due to vendor reporting on adversary behaviors.

In September 2013, Dragonfly began using a new version of this exploit kit, known as the Hello exploit kit. The landing page for this kit contains JavaScript which fingerprints the system, identifying installed browser plugins. The victim is then redirected to an URL which in turn determines the best exploit to use based on the information collected.

Trojanized software

The most ambitious attack vector used by Dragonfly was the compromise of some legitimate software packages. Three different ICS equipment providers were targeted, and malware was inserted into the software bundles they had made available for download on their websites. All three companies made equipment that is used in some industrial sectors, including energy. Delta Electronics, which we cover later in this document, could be subjected to the same malware.

The first identified Trojanized software was a product used to provide VPN access to programmable logic controller (PLC) type devices. The vendor discovered the attack shortly after it was mounted, but there had already been 250 unique downloads of the compromised software.

The second company to be compromised was a European manufacturer of specialist PLC type devices. In this instance, a software package containing a driver for one of its devices was compromised. Symantec estimates that the Trojanized software was available for download for at least six weeks in June and July 2013.

The third firm attacked was a European company which develops systems to manage wind turbines, biogas plants, and other energy infrastructure. Symantec believes that compromised software may have been available for download for approximately ten days in April 2014.

The Dragonfly group is technically adept and able to think strategically. Given the size of some of its targets, the group found a “soft underbelly” by compromising their suppliers, which are invariably smaller, less protected companies. Unauthorized resellers were not examined as part of the analysis nor was the potential for “knock off” companies selling counterfeit hardware.

Delta Elektronics

Intelligence/Reconnaissance:

Russian information on the formation of the companies established under the name of Oleg Vladimirovich Strekozov. Begin dates of the companies and the monies used to create the companies is listed below. Recovered documents indicate other names involved in certain companies under the Oleg name.

(Registration numbers of Russian companies., n.d.)INN – Identifying Tax Number of a tax-payer (consists of 10 digits). Each Russian company has its unique tax number concerning all taxes and duties. Usually, an abbreviation "INN" is used in English letters. INN number is given to a Russian company by the respective state tax body at the moment of company's tax registration in the place of its legal address. As a proof of tax registration, the company receives a certificate with INN issued by the tax body. INN is included in all tax notices and declarations, as well as in Russian bank transfer documents. INN is enough to receive much official info about a Russian company from the Federal Register of Russian companies - "EGRUL."

OGRN

OGRN – Major State Registration Number of the entry made in the Register about the formation of a Russian company (consists of 12 digits). Provided the company was registered before July 1, 2002, OGRN is the number of the entry in the Register about the first filing of information into the Register about the company according to the federal law. Each legal person in Russia has its unique OGRN. OGRN is used in the Register as the number of registration file of a company. As a proof of its OGRN, a company receives the certificate with OGRN issued by the state registration body. OGRN is included into all entries in the Register, all documents issued on specific registration actions. OGRN number lets you receive much official info about a Russian company from the Register.

Company Name	Entry Date	Starting Capital	US Dollars	Date Ended
Autopak-Volga	3/14/2008	10,000 Rubles	\$161.90	3/28/2012
Ayut	5/8/2010	40,000 Rubles	\$647.00	
Delta Elektronics	9/11/2012	20,000 Rubles	\$323.81	
Emilina	8/4/2010	40,000 Rubles	\$647.00	
IntelGrupp	8/12/2010	40,000 Rubles	\$647.00	8/21/2013
Tekstiltorg	8/31/2010	20,000 Rubles	\$323.81	
NIKS	9/6/2010	50,000 Rubles	\$809.52	6/10/2013
Prima	9/9/2010	10,000 Rubles	\$161.90	9/1/2014
Misteriya	9/20/2010	10,000 Rubles	\$161.90	
TDSaturn	9/20/2010	10,000 Rubles	\$161.90	
Magnum	10/12/2010	50,000 Rubles	\$809.52	
Rakurs	6/23/2011	50,000 Rubles	\$809.52	

Nyu-Lajn	7/22/2011	15,000 Rubles	\$242.86
EkonomMarket	8/31/2011	60,000 Rubles	\$971.43
Stroy Holding	9/12/2011	50,000 Rubles	\$809.52
MTK	12/13/2011	20,000 Rubles	\$323.81
Inrost	8/27/2012	20,000 Rubles	\$323.81
Vintazh	11/1/2012	12,000 Rubles	\$194.29
			\$8,530.50

The company stated as running Delta Elektronics is the Matrix Group, LLC. Little information is available at this time on the Matrix Group, LLC. No information exists on this company being created in Russian tax records.

Delta Elektronics and Dragonfly?

Raw data and information review

The last name of Strekozov (СТРЕКОЗОВ) translates to Dragonfly in English. Symantec documented Operation Dragonfly (AKA Energetic Bear) three years ago as a Russian spear phishing organization.

http://www.symantec.com/security_response/writeup.jsp?docid=2014-061601-3811-99&tabid=2

<http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat>

<https://www.f-secure.com/weblog/archives/00002718.html>

(Delta Elektronics, n.d.)Delta Elektronics has two locations in Russia. Saint Petersburg and Moscow.

Address: 105082, Moscow, Semyonov lane, 15, office 615 (Eastern District). Phone: +7 (495) 984-51-05 (Moscow) Phone: 8 (800) 555-90-55 (weekdays from 9:00 to 18:00, a call from the regions of Russia Getting there: 3 minutes walk from the metro station "Semenovskaya."

Address: 195027, St. Petersburg, Shahumyan Avenue, Building 4 (Krasnogvardeyskiy district) Business center "Aurora City," office 320. Metro: Novocherkassk Distance: 10 min. On foot

Email: info@delta-mail.ru and info@delta-electronics.info

The Matrix Group, LLC information:

Phone / fax: +7 (495) 984-51-05 (Moscow) +7 (812) 640-46-90 (St. Petersburg), E-mail: info@matrixgroup.su. © 2004-2012 «Matrix Group."

Treadstone 71 found ties to another company – Vacon (vacon.com and vacon.ru).

Of note, payments for products from Delta Elektronics is by cash courier or via Yandex and WebMoney indicating an organization that is not legitimate.



Establish an initial relationship with a Russian hacker on referenced off vk.com (<https://xakep.ru/>) under and (https://vk.com/xakep_mag) the newly created persona of Oleg Vladimirovich Strekozov.

There are some uncertainty and plenty of leads to follow to be thorough and not leave anything unnoticed. Having said this, the recommendations offered online are valid no matter what further research reveals. If any organizations bought PLCs from either Delta company, better do an emergency security review now.

- Tied to Oleg Strekozov
- One is Delta Elektronics
- Locations in St. Petersburg and Moscow
- Same logo as Delta Electronics – Taipei, Taiwan
- They manufacture PLCs and program them
 - Could Delta Elektronics manufacture the same as knock-offs?
- *“All the IP Addresses and Domains owned by Strekozov Oleg Vladimirovich are known for Zeus, SpyEye, Blackhole, Malware, Crimeware, Scams, and SPAM, etc. Strekozov Oleg Vladimirovich also controls domains within the former Soviet Union TLD.**.su**.”*
- It is highly unlikely that anyone would use their own name assigned to such activities, openly using the name in domain registrations and then openly own over 20 companies (oil and gas) in Russia along with scores of others. It is highly unlikely that someone of that stature in Russia (financial) in and around Moscow, would not show up in people searches using Russian search engines but for domain name registrations – company ownership.
 - Searches on Oleg Vladimirovich Strekozov – finding nothing of direct ties to a person
 - Vladimir Strekozov – retired Russian judge
 - Oleg Strezkozov – aside from hacking sites:
 - <https://www.facebook.com/oleg.strekozov/about>
 - <https://plus.google.com/106396297467067086741/about>
 - <http://vk.com/oledjanqik>
 - <http://loveplanet.ru/page/749987781752/>

- None of which tie to someone old enough and financially viable to own scores of companies.
- *The address given for Oleg in your domain name searches is dead center Red Square - Russia, 107031, Moscow, Proezd Dmitrovskiy 8 (yandex.com – maps)*

<https://www.linkedin.com/company/delta-electronics>

Global HQ – Taipei, Taiwan
 Founded 1971
 Employees 80k
 Revenues \$7B

<http://www.deltaenergysystems.com/en/about-us.htm#tab178>

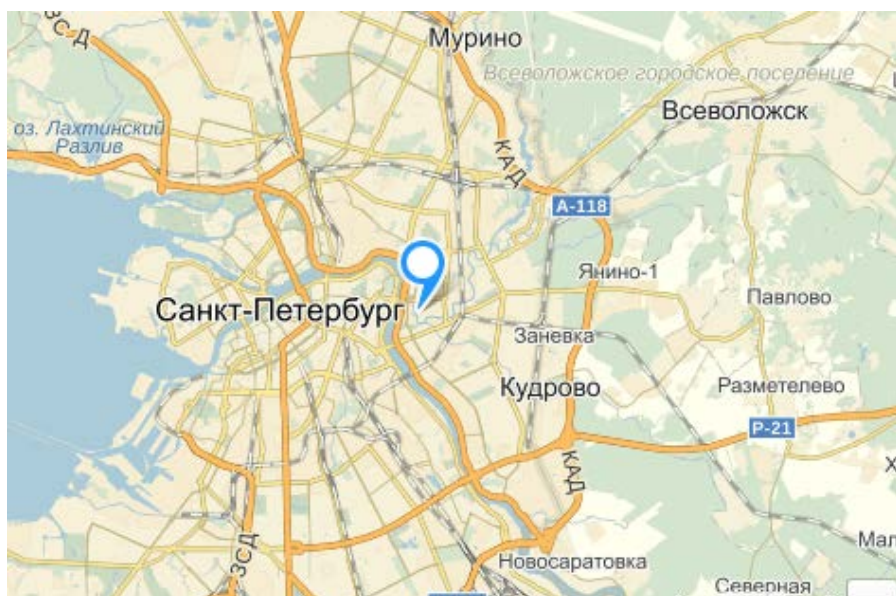
Gaps and Assumptions

Treadstone 71 believes it would be good to know some more details about how PLCs are used in oil and gas transportation. How many are deployed in the typical pipeline? What are key vulnerable points? How many would have to be attacked to create some stoppage for a significant period? Also, it would be very interesting to know about Delta's legitimate business. Who buys from them and with how much volume?

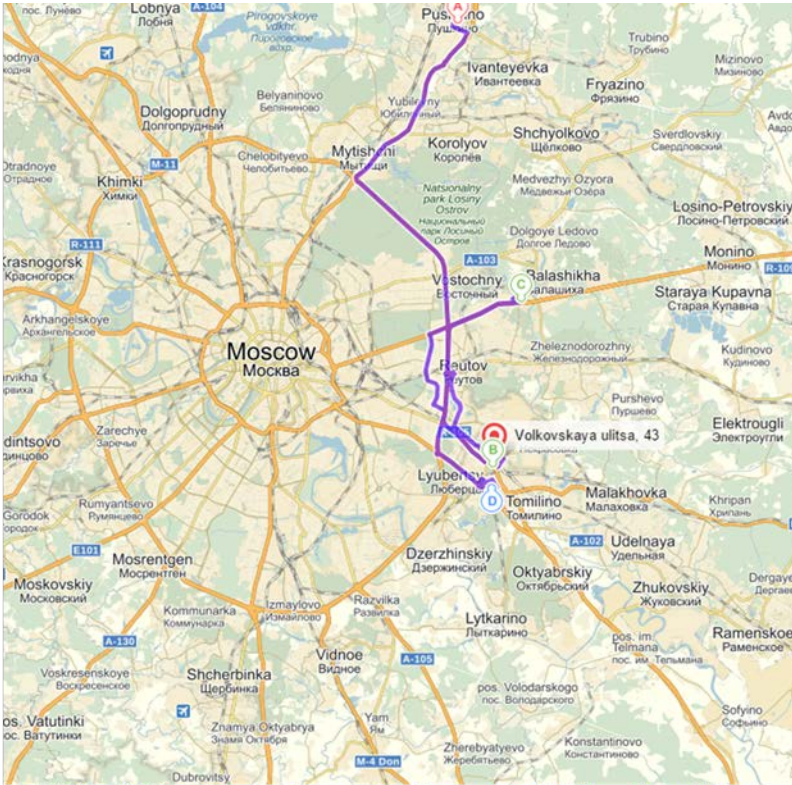
What appears clearly is that there is a bunch of companies registered to this Oleg Strekozov and that his name also appears in some WHOISs about shady sites and that he has some association with malware. Whether he is corporeal or virtual, Mr. Strekozov is associated with Russian cyber organized crime. Treadstone 71 can immediately say that successful organizations of this type are associated with FSB and controlled by oligarchs. Successful oligarchs are close to Putin and, of course, Putin controls the FSB. Real or unreal, Mr. Strekozov is a tool of such a hierarchy.

Treadstone 71 is careful to leap to conclusions about whether Mr. Strekozov is real. He could be a made-up name used for certain registrations, or he could be the weekend doorman at Lubyanka (in jest). But he could be real. His patronymic is Vladimirovich so that the judge could be his father. A look at Facebook finds an Oleg in the Belarusian town of Hlybokaye, educated in eastern Ukraine, about 25 years old. We do not discount him because of age--billions change hands hourly in Moscow, and there are plenty of young criminals driving Maserati's with a bottle of expensive

whiskey in their hand. Real or unreal, S's address of Proezd Dmitrovskiy is in an upscale neighborhood that is also not far from Lubyanka.



- European locations – no mention of Russia
- Asian locations – no mention of Russia
- Several US locations including Houston



- MTK – 140000, Moskovskaya area g Lyubertci, ul Volkovskaya d 43
 - 140000, Московская Арена г Люберцы, ул Волковская д 43
- Inrost – 141206 Moskovskaya area, g Pushkino, Kudrinskoye shosse, d 3
 - 141206 Московская Арена, г Пушкино, Кудринское шоссе, д 3
- Delta Elektroniks – 143903 Moskovskaya area, g Balashiha, ul Valdimirskaya, d 139
 - 143903, Московская Арена, г Балашиха, ру Владимирская, д 139
- Vintazh – 140006 Moskovskaya area, g Lyubertci, ul Yuzhnaya, d 26 A
 - 140006 Московская Арена г Люберцы, ул Южная, д 26 А

although the coordination and precision for this to work past a few days would be extraordinary.

Another possibility is that this is just a scheme for some oligarchs to make money. They speculate on buying a tanker filled with crude. While tanker is at sea, an incident occurs at some pipeline or port spiking the price of oil and Oleg's tanker pulls into Rotterdam right at the peak.

Finally, this could be just a part of a Russian medium-term strategy to contaminate as much hardware, firmware, and software as possible.

- Name of Delta Electronics
- Address Moscow, Semenovskiy per., 15, of. 615
- Email info@deltaelectronics.su
- Section Industrial equipment
- Phone:+7 (495) 9845105, 8 (800) 5559055 - Different locations than that of Oleg's site for Delta Elektroniks –

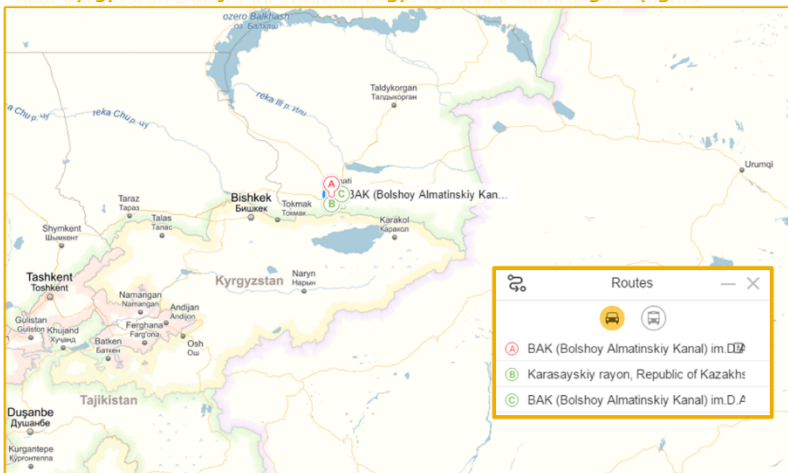
Delta or Delta? The more Treadstone 71 investigates on this company, the more skeptical we have become about the innocence of the Taiwanese company. We have found that the Russian Delta has attended trade shows and held press conferences. With thousands of dollars of sales and only a limited number of companies that make PLCs, do we believe that some people in Taipei are unaware about this? Treadstone 71 has discovered other companies that do business in Russia but try not to advertise that in the West. Could it be that Delta-Ru is buying or arranging sales and Delta-Tai is happy to turn away from this? The price for doing such business in and through Russia is, of course, to take Russian partner. Either way, the possibility of supply chain contamination is real.

In applying an informal analysis of competing for a hypothesis to all this, Treadstone 71 has come up with two more hypotheses that fit the facts (as they stand now, understanding that more information and analysis is needed).

This could be an effort to cause serial failures that could drive up energy prices,

- Oleg does not show up in any people searches in Russia yet appears as a hacker and as an owner of scores of companies. Is it likely that this can be both accurate and true?
 - Treadstone 71 does not believe this is true.
- Gazprom has direct operations in Kyrgyzstan
- Oleg Vladimirovich Strekozov does not seem to exist
- Vladimir Strekozov was a constitutional court judge – hardly a hacker
 - Not the same as Oleg Vladimirovich Strekozov
 - Any searches of Oleg Strekozov about Oil and Gas only brings up site registration
 - No mention of someone who owns so many firms in and around Moscow (expensive)

Other Oleg oil and gas companies near Kyrgyzstan – Major location for Krgyz to Uzbek natural gas 'spigots'



<http://oilprice.com/Energy/Natural-Gas/What-Part-Did-Russia-Play-In-Kyrgyzstan-Uzbekistan-Gas-Dispute.html> and <http://www.eurasianet.org/taxonomy/term/3756>

- No mention of someone who owns first in the Kyrgyz area related to Gazprom

- It is more likely that Oleg Strekozov is just a name backed by Russian government funding. The location is Red Square. “Thumbing their nose.”

- Question: Why duplicate Delta Electronics if they are not the same company?

- What could the motivation for Russia be to pose as Delta Electronics?

- Hardware used in gas and oil production

- Sold in international markets – global name – accepted – trusted

Treadstone 71 can imagine all kinds of functions that could be contaminated with logic bombs and backdoors, ready for the call of the Rodina (Russian Motherland).

It should be noted that these three hypotheses are not mutually exclusive of one another as the motivations could logically coexist.

Analysis of Competing Hypotheses I

	Type	Credibility	Relevance	H: 1	H: 2	H: 3	
				Delta Elektroniks is a front company used by Russian intelligence/nation state actors to infect energy organizations for cyber espionage and/or sabotage.	Delta Elektroniks is a front company used by a criminal group to either defraud energy companies by providing fraudulent equipment or "skim off the top".	Delta Elektroniks is a legitimate provider of SCADA equipment, possibly using the Delta Elektroniks name to increase its chances of success.	
				-4.707	-4.828	-20.242	
	Enter Evidence						
E13	The "secure facility" in E12 may be a government building. "We plotted the companies identified on a Yandex map showing the proximity of these organizations to one another and in proximity to known state-run intelligence organizations in Moscow. All are located inside the Moscow loop, some occupying the same building complex."	Observation of picture and report from Treadstone 71	MEDIUM	HIGH	CC	II	I
E15	2 of Oleg Vladimirovich Strekozov's 18 registered companies generated revenue (60-70K), but all of the others have 0 or little revenue.	Org-info	HIGH	HIGH	I	CC	I
E14	VK profile of Oleg Vladimirovich Strekozov has just an image of someone with an Anonymous mask (possible front?)	VK	HIGH	HIGH	I	N	I
E7	The Taiwanese Delta Elektroniks website does not show an official office or outlet in St. Petersburg (only one in Moscow).	Delta Elektroniks website.	HIGH	HIGH	C	C	II
E21	Timeline shows that "Delta Elektroniks" was created in 2002, and that the Matrix and "Delta Elektroniks" websites were created in 2008 and 2009, respectively. The legitimate Delta Elektroniks was founded in 1971, and the website was created in 2001.	Internet research	HIGH	HIGH	C	C	I
E19	To date, there have been no known issues with the "Delta Elektroniks" parts that have been installed.	Conversation with stakeholders.	LOW	MEDIUM	I	C	C
E18	Vacon-ru.com is also registed by YURI YAKOVLEV and is also associated with The Matrix, and claims to be a supplier of Vacon equipment from Danfoss (Finland). However, the real Danfoss site appears to have no connection to The Matrix, and does not list the Matrix as a supplier. Vacon-ru appears to be ripping off the real Danfoss/Vacon products.	Research of websites	MEDIUM	HIGH	C	C	I
E17	The legitimate Delta Elektroniks (Taiwan) does mention using The Matrix as a supplier.	Internet research	MEDIUM	HIGH	C	C	I
E12	The name Oleg Vladimirovich Strekozov does not appear to belong to a person with a substantial online presence, aside from a mostly empty VK profile.	Internet research	LOW	HIGH	C	C	I
E11	A business address found in the metadata appears to a secure facility with barbed wire fences, no logos/signs, etc.	Google Maps	HIGH	HIGH	CC	I	C
E9	The Russian "Delta Elektroniks" website includes links to the official Taiwanese Delta Elektroniks page (but not vice versa) and includes a page with a bio of the correct Delta Elektroniks CEO	"Delta Elektroniks" website	HIGH	HIGH	C	CC	I
E8	The format of the Russian "Delta Elektroniks" website is different from the official Delta Elektroniks website.	"Delta Elektroniks" website	HIGH	LOW	N	C	I
E5	The name "Oleg Vladimirovich Strekozov" is listed in the whois information for several IP addresses that conducted cybercriminal "botnet activity" (spam, etc.)	Multiple sources (vendor reports, user forums, etc.)	HIGH	HIGH	C	CC	I
E20	Signs on the building said "Brand Store" and "Micromachines" in Russian.	Google Maps	HIGH	MEDIUM	N	C	C
E16	Several related sites, including the website of the company listed as the supplier (The Matrix) are all registered by the same name: YURI YAKOVLEV.	Observations of "Delta Elektroniks" sites and matrixgroup.su, and whois info.	HIGH	MEDIUM	C	C	N
E10	The Russian "Delta Elektroniks" website does not take payments; when you add items to your cart, you must fill out a contact form and "send an inquiry".	"Delta Elektroniks" website	HIGH	LOW	C	C	C
E6	Both the Karagany Trojan and BlackEnergy malware, which were used in cyber espionage and sabotage campaigns targeting the energy sector, were made available in underground forums (source code leaks) many years ago (e.g., Karagany in 2010).	Multiple sources (vendor reports)	HIGH	HIGH	N	C	NA
E4	Стрекоза (Strekozov - Oleg's last name) means "dragonflies" in Russian (Symantec named the Havex campaign targeting energy organizations "Dragonfly")	Translation of Russian	HIGH	LOW	C	NA	NA
E3	Russian nation state campaigns targeting energy organizations used supply chain as an attack vector (watering hole attacks). The threat actors compromised vendor sites and replaced software installers with Trojanized versions that provided the attackers VPN access to the PLCs.	Symantec	MEDIUM	HIGH	CC	C	NA
E2	Russian nation state campaigns targeting energy organizations targeted ICS systems (including PLCs) via phishing, exploit kits, and watering hole attacks.	Multiple sources, including reliable government sources	HIGH	HIGH	C	N	NA
E1	Russian nation state actors frequently conduct cyber espionage and/or sabotage campaigns targeting Energy companies in the US, Europe, and Ukraine.	Multiple sources, including reliable government sources	HIGH	HIGH	C	NA	NA

Analysis of Competing Hypotheses II

	Type	Credibility	Relevance	H: 2	H: 3	H: 1	H: 5	H: 4
				Delta Elektronics is a fake company set up by a nation state for a foothold in world wide energy sector.	Delta Elektronics has been a knock off company the whole time for monetary gain for cyber criminals	Delta Elektronics is a legitimate reseller of Delta Electronics Hardware	Delta Elektronics is performing corporate espionage	Energetic Bear is revamping an attack using Delta Elektronics PLCs
	Weighted Inconsistency Score ⇄			-2.0	-6.0	-9.914	-10.656	-11.656
	Enter Evidence							
E12	Delta Elektronics located near various Russian state run intel orgs	Report/Maps	HIGH	LOW	I	I	I	I
E16	DragonFly is a spearphishing campaign	Report	HIGH	LOW	I	I	C	I
E7	Blackenergy/Energetic bear attacks scada elements in 2014	Report	HIGH	LOW	C	I	I	C
E6	Strekozov translates to "dragonfly"	translator	HIGH	LOW	C	I	I	C
E11	Business profile sites mention Oleg Strekozov	Web search	HIGH	HIGH	C	NA	I	I
E10	Deltaww does not directly refer to D.EK	Website	HIGH	HIGH	C	I	C	NA
E9	Multiple domains under "Delta" brand	Research	HIGH	MEDIUM	C	N	I	I
E5	delta elektroniks shares infrastructure with Matrix Group, LLC	Website	HIGH	MEDIUM	C	N	I	I
E4	Delta Electronics is a subsidiary of Matrix LLC	Website	HIGH	MEDIUM	C	N	I	I
E3	Oleg owns multiple businesses in the energy sector	Report	HIGH	MEDIUM	C	N	I	I
E2	Delta Elektronics accepts unusual payment types (Web Money, Cash Courier)	Report	HIGH	HIGH	C	C	I	N
E14	PLCs are easily programmed	Wikipedia	HIGH	MEDIUM	C	N	I	C
E8	Past IP address reported as malicious belonging to Strekozov	Website	LOW	LOW	C	N	I	C
E15	Social media sites for "oleg" show individuals not capable of sophisticated attack	social media	LOW	MEDIUM	N	N	N	N
E13	Vladimir Strekozov is may be a Russian intel	Records	MEDIUM	LOW	N	N	N	N

In Summary

Although there is an absence of evidence supporting a direct alignment of BlackEnergy, Dragonfly, and Delta Elektronics, 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 Elektronics may be limited in a “Dunbar’s number” method of maintain secrecy.

Although there is an absence of evidence supporting a direct alignment of BlackEnergy, Dragonfly, and Delta Elektronics, 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 highly 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 Elektronics may be limited in a “Dunbar’s number” method of maintain secrecy.

Treadstone 71 Proprietary and Confidential



We cannot rule out direct Russian involvement based upon previous judgments and behaviors by the Russian government and Russian proxies. Historical profiling of Russian activities indicates at a minimum, their participation in these activities.

Adversary intent, whether it is BlackEnergy, Dragonfly, or Delta Elektronics combined with expert capabilities enables a high probability of threat. Additionally, the probability of threat occurrence in unison with the success of the actions and the overall impact(s) when examined considering the Ukrainian attacks, represents an elevated level of risk.

The use of hybrid warfare methods in combination with constantly moving attack vectors makes difficult, attribution and methods of defense. The adversary(s) behind the actions demonstrate information superiority while revealing behaviors with similarities. Continued data and information collection for analysis is required but serves as a double-edged sword. This sword ensures we continue to churn examining multiple different versions of information using limited resources while missing the primary intent and potentially simple conclusion as to the intent and success of the adversary(s).

Search results for *host:216.58.213.132*

Multi-Process	Net
Extracted Files	Carv

[Download all DNS Requests \(CSV\)](#) [Download all Contacted Hosts \(CSV\)](#)

▲ Timestamp

Details

August 25 2017, 14:59 (CEST)	Input Delta_WPLSoft_V2.30.exe PE32 executable (GUI) Intel 80386, for MS Windows c31bf30a29d19785577100e9e0c4206f901ca3bfa651d7cfc68f718b02de9d7e
	Threat level malicious
	Summary Threat Score: 62/100 AV Multiscan: 1% Sandrator.c Matched 31 Signatures
	Countries
	Environment Windows 7 32 bit
	Action Re-analyze
August 25 2017, 14:59 (CEST)	Input bad51b2a246f4fb71bd6bc4f054e1b5972184c9f04041e3616783ba45ef24076 PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extra ... bad51b2a246f4fb71bd6bc4f054e1b5972184c9f04041e3616783ba45ef24076
	Threat level malicious
	Summary Threat Score: 100/100 AV Multiscan: 15% ML.Attribute Matched 64 Signatures
	Countries
	Environment Windows 7 32 bit
	Tags coinminer dofail miner sharik smokeloader
	Action Re-analyze

Infection Examples

August 25 2017, 14:50 (CEST)	Input g2CP.zip PE32 executable (GUI) Intel 80386, for MS Windows a6f1bad31d79f46b2a6d53d6be87e8c01f9819fbf541f240584dc49b0256fb51
	Threat level malicious
	Summary Threat Score: 100/100 AV Multiscan: 20% ML.Attribute Matched 50 Signatures
	Countries
	Environment Windows 7 32 bit
	Tags ransomware
	Action Re-analyze

- <https://www.hybrid-analysis.com/sample/5e0c99e6350fd89a7b0d2dd480873ef2f2f566b8a41848a794cc7fa458c0a7ad?environmentId=100>
- <https://www.reverse.it/sample/41cc903cd5fa2516855cffc80ae5724a3fffee795c79aa81ea136e94db2bd34f?environmentId=100>
- <https://malwr.com/analysis/NzgzZmRhZjM5Mjc2NTg1ODY1ZTQxYzNkYWRIYjU/>

August 25 2017, 14:28 (CEST)

Input WinToUSB_Free.exe
PE32 executable (GUI) Intel 80386, for MS Windows
db02057c3f23fbd9ec8ac198a0523cf18fca859b974e02ddaf150609c54730e9

Threat level malicious

Summary Threat Score: 100/100
AV Multiscan: **Marked as clean**
Matched 72 Signatures

Countries 

Environment Windows 7 32 bit

Action

August 25 2017, 14:25 (CEST)

Input GUIAtrtjGTUFGjKx.bat
ASCII text, with very long lines, with no line terminators
ae554c3c7094f0f6d0d5e8f4664614dd10a87a5e39d192f25daeba31c46a7c5e

Threat level malicious

Summary Threat Score: 100/100
AV Multiscan: 25% Generic.PwShell.Rozena.1
Matched 26 Signatures

Countries  

Environment Windows 7 32 bit


Action

August 25 2017, 14:24 (CEST)

Input 20170825_ID904754594.vbs
ASCII text, with CRLF line terminators
21207599eedb3ad315571fadcd3d843fbe2e213f1c9970208612a7834b170b55

Threat level malicious

Summary Threat Score: 100/100
AV Multiscan: 25% Mal_VBSCRDLX
Matched 64 Signatures

Countries    

Environment Windows 7 32 bit

Tags locky ransomware

Intelligence

August 25 2017, 14:41 (CEST)

Input msg0854.rar
ASCII text, with CRLF line terminators
35a2ec27bbda54070eb83f8413f7cdd5c74a2ba6f0daab334a0f5ed4c8eba94f

Threat level malicious

Summary Threat Score: 100/100
AV Multiscan: 26% Mal_VBSCRDLX
Matched 27 Signatures

Countries    

Environment Windows 7 32 bit


Action

August 25 2017, 14:31 (CEST)

Input WinToUSB_Setup.exe
PE32 executable (GUI) Intel 80386, for MS Windows
7f5d9060da87b64c0f91b31d8a211e0d86e69b23a8ab460743a86297974bbd62

Threat level malicious

Summary Threat Score: 100/100
AV Multiscan: **Marked as clean**
Matched 72 Signatures

Countries 

Environment Windows 7 32 bit


Action

August 25 2017, 14:30 (CEST)

Input WinToUSB_Free.exe
PE32 executable (GUI) Intel 80386, for MS Windows
cb20635582fcb4b0d54b2e6f60955303b0505748cc787bff90cbebf83f911a8c

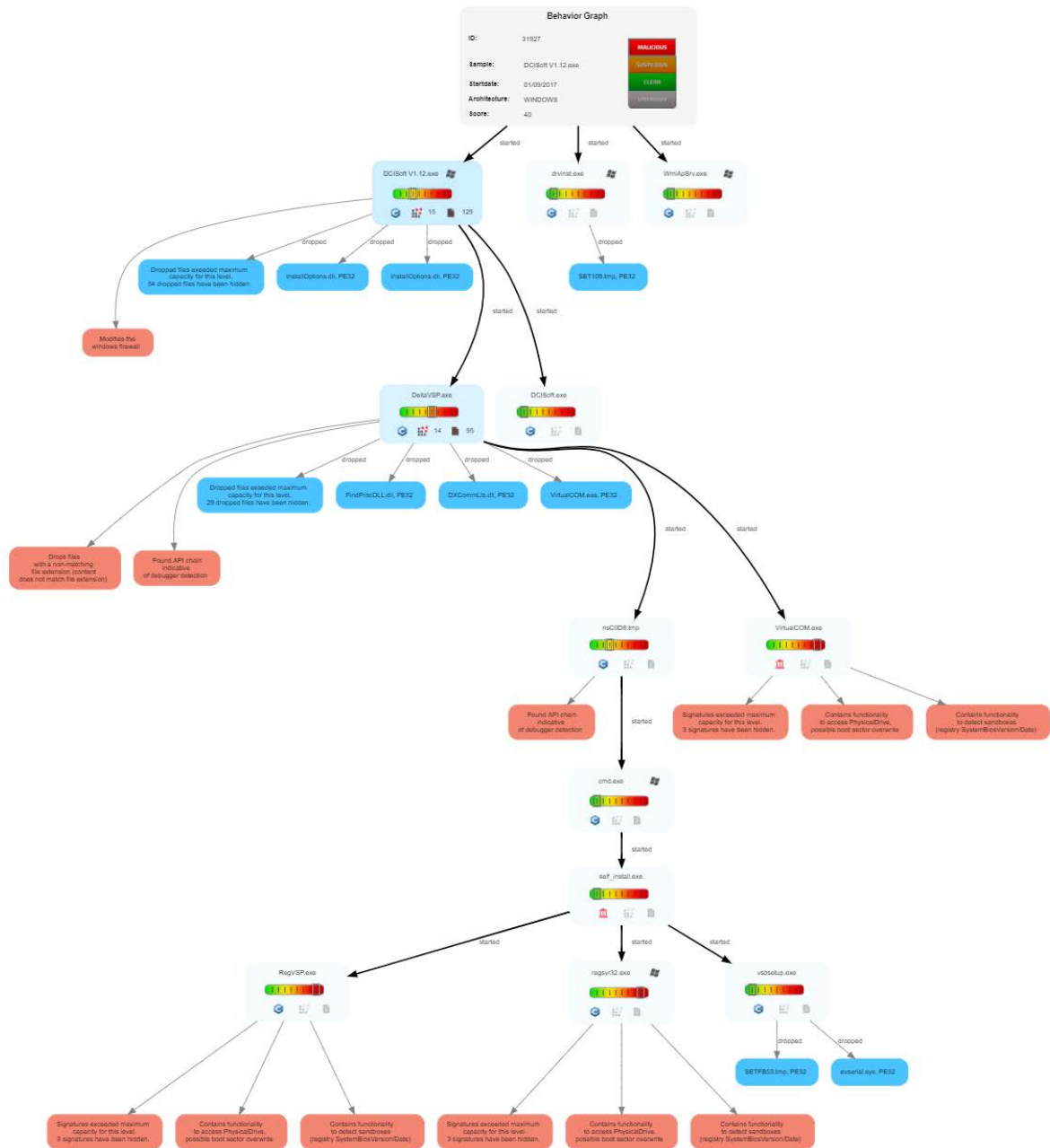
Threat level malicious

Summary Threat Score: 100/100
AV Multiscan: **Marked as clean**
Matched 64 Signatures

Countries 

Environment Windows 7 32 bit

Action



Search Criteria Example:

site:.com | .edu | .org | .uk | .net | .gov | .mil | .su | .ru | .tw | .ir dcisoft_v1.12

2 可程式控制器 (1161)







3 -- 請選擇 --

- 型錄
- 技術文件
- 操作手冊
- 應用手冊
- 安裝手冊
- 連線手冊
- 選購配備
- 軟體
- 尺寸圖
- 安規證書
- 電子參數檔
- 軟體








開始搜尋

軟體

AH系列PLC

軟體名稱	說明	適用機種	作業系統	發行日期	檔案大小	註解	檔案
PLC編輯軟體							
ISPSOFT V3.02	PLC編輯軟體	AH系列、AS系列及DVP系列PLC	Windows® XP/Vista/7 (32-bit/64-bit)/8/10(64-bit)	2016/07/25	472MB	通訊功能需搭配安裝 COMMGR	
ISPSOFT V3.03	PLC編輯軟體	AH系列、AS系列及DVP系列PLC	Windows® XP/Vista/7 (32-bit/64-bit)/8/10(64-bit)	2017/06/19	467MB	通訊功能需搭配安裝 COMMGR	
COMMGR V1.07	通訊管理軟體	AH系列、AS系列及DVP系列PLC	Windows® XP/7(32-bit/64-bit)/8/10 (64-bit)	2016/12/14	16.9MB	-	
COMMGR V1.06	通訊管理軟體	AH系列、AS系列及DVP系列PLC	Windows® XP/7(32-bit/64-bit)/8/10 (64-bit)	2016/07/25	18.6MB	-	
運動控制編輯軟體							
PMSOFT V2.10	運動控制器編輯軟體	AH系列與DVP系列運動控制器	Windows® XP/Vista/7(32-bit/64-bit)/8(64-bit)	2014/11/18	121MB	通訊功能需搭配安裝 COMMGR	
PMSOFT V2.09	運動控制器編輯軟體	AH系列與DVP系列運動控	Windows® XP/Vista/7(32-bit/64-bit)/8(64-bit)	2014/11/18	121MB	通訊功能需搭配安裝 COMMGR	

DVP Series PLC

Software Name	Description	Supported Device	Operating System	Issue Date	File Size	Comment	File
PLC Programming							
COMMGR V1.07	Communication management software	AH series, AS series and DVP series PLCs	Windows® XP/7(32-bit/64-bit)/8/10(64-bit)	2016/12/14	16.9MB	-	
COMMGR V1.06	Communication management software	AH series, AS series and DVP series PLCs	Windows® XP/7(32-bit/64-bit)/8/10 (64-bit)	2016/07/25	18.6MB	-	
ISPSOft V3.02	PLC programming software	AH series, AS series and DVP series PLCs	Windows® XP/Vista/7 (32-bit/64-bit)/8/10(64-bit)	2016/07/25	472MB	Please use with COMMGR for communication function	
ISPSOft V3.03	PLC programming software	AH series, AS series and DVP series PLCs	Windows® XP/Vista/7 (32-bit/64-bit)/8/10(64-bit)	2017/06/19	467MB	Please use with COMMGR for communication function	
WPLSOft V2.42	PLC programming software	DVP series PLCs	Windows® XP/Vista/7(32-bit/64-bit)/8/10(64-bit)	2016/03/11	72.6MB	-	
WPLSOft V2.45	PLC programming software	DVP series PLCs	Windows® XP/Vista/7(32-bit/64-bit)/8/10(64-bit)	2017/06/21	75.9MB	-	
Network							
CANopen Builder V6.00	CANopen configuration software/motion control programming software	AH series CANopen modules, DVP series built-in CANopen PLCs, DVP series CANopen modules, DVP-MC motion controller	Windows® XP/7(32-bit/64-bit)/8(32-bit/64-bit)/10(64-bit)	2017/07/24	377MB	-	
	CANopen configuration	AH series CANopen modules, DVP series built-	Windows® XP/7(32-				

Download Software

File Size	Issue Date	Operating System	Explanation	Software Name
1A.9KB	2011-11-16	(Windows V (32bit	IFD9Δ=3 Drivers	IFD9Δ=3 Drivers
324MB	2014-09-24	Windows 2000, XP, Vista or Windows V (32-bit/64-bit	Editing software for DVP series and AHΔ=0 series (Multilingual) Note: please use with COMMGR for communication function	ISPSOft V2.0Δ
MB 19.Δ	2013-11-21	(Windows XP, V (32-bit/64-bit	Monitor AH series by SCADA/OPC client(Trial (version for 30 mins NOTE: please install OPC Core Components before installing Delta OPC .quick start for details	Delta OPC V1.00
244MB	2015-02-13	Windows XP(32-bit), Windows V(32-bit/64-bit	PROFIBUS DP configuration software	SYCON.net V1.3Δ
20.9MB	2015-02-09	Windows XP, Windows V(32-bit/64-bit), (Windows A(32-bit/64-bit	CAN bus Message Analysis Software (for all (IFD9Δ=3 firmware versions	NetView Builder V2.02
13ΔKB	2012-06-19	(Windows XP, Windows V(32-bit/64-bit	USB driver for DVP-SE	DVP-SE USB Driver
4.04MB	2012-06-19	(Windows XP, Windows V(32-bit/64-bit	DVP-SX2 driver	DVP-SX2 Driver
10.9MB	2013-02-23	(Windows XP, Windows V(32-bit/64-bit	integrated communication management software	COMMGR V1.0F

Industrial Automation

8 800 555 90 55

ПРИБОРЫ И СРЕДСТВА ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ СО СКЛАДА В МОСКВЕ И С-ПЕТЕРБУРГЕ

DELTA ELECTRONICS, INC.

Программируемые контроллеры, Delta



DELTA ELECTRONICS | ИНЖИНИРИНГ | ПРИВОДНАЯ ТЕХНИКА | ПРЕОБРАЗОВАТЕЛИ ЧАСТОТЫ | ФОРУМ |

- Средства автоматизации
- Программируемые логические контроллеры DVP
- Панели оператора
- Программируемые реле
- Температурные контроллеры
- Счётчики / Тахометры
- Таймеры / Реле времени
- Твердотельные реле
 - твердотельные реле - Fotek
 - твердотельные реле Sipin
 - твердотельные реле Greegood
- Регуляторы мощности
 - регуляторы мощности SIPIN
 - регуляторы мощности Fotek

- Базовые блоки контроллеров серии **ES** со встроенным интерфейсом RS-232 и RS-485;
- Базовые блоки контроллеров серии **EX** со встроенным интерфейсом RS-232 и RS-485;
- Модули расширения цифровых входов/выходов для контроллеров серии **ES-EX**;
- Базовые блоки контроллеров серии **SS** со встроенным интерфейсом RS-232 и RS-485;
- Базовые блоки контроллеров серии **SA** со встроенным интерфейсом RS-232 и RS-485;
- Модули расширения цифровых входов/выходов для контроллеров серии **SS, SX** и **SA**;
- Базовые блоки контроллеров серии **SX** со встроенным интерфейсом RS-232 и RS-485;
- Базовые блоки контроллеров серии **EC**;
- Базовые блоки контроллеров серии **EH(EH2)** со встроенным интерфейсом RS-232 и RS-485;
- Модули расширения цифровых входов/выходов для контроллеров серии **EH(EH2)**;
- Дополнительное оборудование для контроллеров серии **EH**;
- Базовые блоки контроллеров серии **SV (во многом аналог EH)**;
- Дополнительное оборудование для контроллеров серии **SV**;
- Базовые блоки контроллеров серии **PM**;
- Дополнительное оборудование для контроллеров **DVP**;
- Универсальные конвертеры интерфейса (**не только для DVP**);
- Документация **Руководство по программированию контроллеров DVP**;

ПЛК Delta - Price List (Цена)

26.09.2016 - Новости европейского представительства Delta Electronics



Вышла статья в отраслевых новостях ассоциации пользователей CAN об удаленном управлении приводами C2000 и CP2000 по протоколу CANopen. Текст статьи на английском доступен на сайте

Контакты**О нас****Новости**

Новости от

[производителей](#)[Специальные](#)[предложения](#)[Новости мира QNX](#)[Будни системной](#)[интеграции](#)[Новости RTS](#)**Продукты****Услуги****Сделано в RTS****Статьи****Проектантам****Партнеры**[Главная страница](#) > [Новости](#) > [Апрельский выпуск новостей на английском языке от Delta Electronics](#)

Апрельский выпуск новостей на английском языке от Delta Electronics



08.04.2016 14:53

Предлагаем вашему вниманию апрельский выпуск новостей Delta Electronics на английском языке. В выпуске информация о сертификации ПЧ Delta VACnet, вступление Delta в PLC Open, многочисленные обновления версий ПО и firmware с новым функционалом, описание приложений, ЧaBo

Подробнее:

- Delta Electronics принимает участие в выставке Middle East Electricity в Дюбаи
- Delta Electronics принимает участие в промышленной выставке Hannover Messe в Ганovere
- Вышла статья в отраслевых новостях ассоциации пользователей CAN об удаленном управлении приводом C2000 с помощью CAN
- CP2000 прошел сертификацию VACnet и опубликован в официальном реестре лаборатории BTL
- Delta Electronics стала официальным членом PLC Open (www.plcopen.org)
- Изменились разъемы платы управления рекуператором REG2000
- Обновилась прошивка VFD-EL, уточнены некоторые функции, связанные с PID, каскадным управлением насосами, внешним управлением ПЧ по MODBUS
- По требованию стандартов Евросоюза, США, Китая и Тайваня, максимально возможная частота серии VFD-EL ограничена 599Гц (было 600 Гц).
- Delta расширила линейку блоков питания новой, сверхкомпактной серии Sync до 50Вт и 100Вт. Миниатюрные блоки питания имеют высоту всего 75 мм и толщину 35 мм, работают от -40С, оснащены сухим контактом готовности, имеют

Новости

Встречайте новый преобразователь частоты CFP2000 от Delta Electronics, которому не нужен шкаф

12, Июнь 2017

Много интересного и нужного в новом приводе для машиностроения Delta Electronics

15, Апрель 2017

Модульный HMI серии TPC-5000 от Advantech - современный и удобный конструктор решений HMI для индустрии 4.0

19, Март 2017

Подписаться на RSS

Подписка на рассылку новостей [Архив новостей](#)



Авторизованный дистрибьютор компаний:
DELTA ELECTRONICS, AUCOM и FOTEK

О КОМПАНИИ

НОВОСТИ

СТАТЬИ

ПРОДУКЦИЯ

ПОДДЕРЖКА

КОНТАКТЫ

- О компании
- Новости
- Статьи
- Продукция
- Поддержка
- Контакты



Акции!



Новости

Новости



14.04.2014 - Снижение цен на преобразователи частоты Delta Electronics



Следуя потребностям российского рынка, с 1 апреля 2014 авторизованный российский дистрибьютор средств промышленной автоматизации Delta Electronics значительно снизил цены трехфазных векторных преобразователей частоты серии VFD-E в диапазоне мощностей 5,5-22 кВт.

10.04.2014 - Приглашаем на выставку с нашим участием «КранЭкспо-2014»



Дата проведения выставки: с 23 по 25 апреля 2014 года
Место проведения: г. Москва, ВВЦ, пав. 75
Номер стенда: D102

08.04.2014 - Новые модели в серии простых компактных преобразователей частоты.



Серия VFD-L пополнилась моделями на 1,5 и 2,2 кВт в классе напряжения 220В.
Дополнительную информацию по новым моделям смотрите далее.

08.04.2014 - Участие Delta Electronics в конференции на Ишимбайском станкоремонтном заводе




В рамках проводившейся в столице Башкортостана г. Уфе выставки «Промэкспо, станки и инструменты» 19 марта 2014 года состоялась выездная конференция, организованная Ишимбайским станкоремонтным заводом, в ходе которой от компании Delta Electronics были представлены доклад и презентация.



Комплексные поставки средств автоматизации от Матрикс Групп

8 800 555 90 55

- Ваша корзина
- Каталог товаров
- + Электропривод
- + Сервопривод
- + Регуляторы мощности
- + Твердотельные реле
- + Панели оператора
- + Контроллеры (PLC)
- + Приборы
- + Энцикодеры
- + Датчики
- Мотор редукторы
- ИБП - Источники бесперебойного питания
- Доставка и оплата
- Статьи
-  Карта сайта
- Форум - Delta Electronics

[Каталог товаров](#) | [Каталог сайтов](#) | [Контакты](#)

DVP (Delta)

DVP-SS

Стандартная серия, гибкое расширение

- Сверхкомпактная серия
- ЦПУ: 14 точек дискретного ввода/вывода (8DI + 6DO)
- Модули расширения на 8 и 16 точек ввода/вывода
- Модули аналогового ввода/вывода
- Два встроенных коммуникационных порта
- Большое количество инструкций
- Высокоскоростные входы/выходы
- Низкая стоимость

Название	Цена	Количество
DVP14SS11R2 14 Point, 8DI, 6DO (Relay), 24V DC Power, SLIM	3200	
DVP14SS11T2 14 Point, 8DI, 6DO (Transistor), 24V DC Power, SLIM	3200	

[Посмотреть заказ](#)



21.01.2017 - Старт продаж преобразователей частоты



Ст
пр
EM
Ст
пр
EM
Ст

SINEE серии EA100

Серия компактных преобразователей частоты с высокой стабильностью работы и простыми применениями с вентилями простыми машинами.

EM303B Векторный преобразователь частоты

Основные преимущества V/F и управления скоростью и моментом: автоматическая настройка двигателя, стандартный встроенный потенциометр и работа с нормальной и тяжелой нагрузкой. Встроенный ПИД-регулятор скорости, высокая точность. Встроенный тормозной диод опционально для моделей 22-400W. Автоматический поиск скорости, автоматический поиск момента, фланцевое крепление, режим многофункциональных приложений.

Bibliography

- Aapo Cederberg and Pasi Eronen*, "How are Societies Defended against Hybrid Threats?" Geneva Centre for Security Policy, September 2015. (<http://www.gcsp.ch/News-Knowledge/Publications/How-are-Societies-Defended-against-Hybrid-Threats>); Keir Giles, "Western Media Must Get Creative in Infowar," The Moscow Times (Russia), August 4, 2015.
- András Rácz*, "Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist," The Finnish Institute of International Affairs, June 16, 2015. (http://www.fiia.fi/en/publication/514/russia_s_hybrid_war_in_ukraine/)
- Antiy*. (n.d.). Comprehensive Analysis Report on Ukraine Power System : <http://www.antiy.net/p/comprehensive-analysis-report-on-ukraine-power-system-att>
- Douris, C.* (2017, January 9). *Cyber Threats to the U.S. Electric Grid Are Real*. Retrieved from The Buzz: <http://nationalinterest.org/blog/the-buzz/cyber-threats-the-us-electric-grid-are-real-19000>
- Delta Elektronics*. (n.d.). Cyber Shafarat: <https://treadstone71llc.files.wordpress.com/2016/04/delta-elektroniks.pdf>
- DLELY Key Statistics - Delta Electronics Inc.* (2017, January 15). Delta Electronics Inc.: <http://www.marketwatch.com/investing/stock/DLELY/profile>
- Dragonfly vs. America, Courtesy of Russia : <http://founderscode.com/dragonfly-vs-america-courtesy-of-russia/>
- Dragonfly*. (n.d.). Western Energy Companies Under Sabotage Threat : <https://malwaretips.com/threads/dragonfly-western-energy-companies-under-sabotag>
- Energy Sector Alert*. (n.d.). Dragonfly Attack /: <http://www.isssource.com/energy-sector-alert-dragonfly-attack>
- JohnIB*. (n.d.). Russian hackers penetrated US electricity grid: <https://johnib.wordpress.com/2016/12/31/russian-hackers-penetrated-us-electricit>
- Keir Giles, Philip Hanson, Roderic Lyne, James Nixey, James Sherr, and Andrew Wood*, "The Russian Challenge," Chatham House, June 2015, (https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20150605RussianChallengeGilesHansonLyneNixeySherrWood.pdf)
- Mazarr, M. J.* (2015). *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. Strategic Studies Institute.
- Registration numbers of Russian companies*. (n.d.). INN number: <http://intranorm.com/en/comm/ogrn-and-inn-en.html>
- Star Report*. (n.d.). Dragonfly Cyberespionage Attacks - HITECH : <http://research.hitechanswers.net/content41603>
- Symantec*. (n.d.). Backdoor.Oldrea and Trojan.Karagany : <https://community.mcafee.com/thread/70047?start=0&tstart=0>
- Timeline: Ten Years of Russian Cyber Attacks on Other*. (n.d.). NBC News: <http://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-c>
- WHEN THE LIGHTS WENT OUT*: <http://docplayer.net/31222353-When-the-lights-went-out-a-comprehensive-review-of>

Reliability and Validity Rating Scales

Source Reliability

A Completely Reliable	<ul style="list-style-type: none">• No doubt of trustworthiness, authenticity• The source is competent• History of the source is completely reliable
B Usually Reliable	<ul style="list-style-type: none">• Some doubt of trustworthiness, authenticity• Some doubt about competence• Majority of the time a reliable source
C Fairly Reliable	<ul style="list-style-type: none">• Usually some doubt of authenticity, trust• Usually some doubt about competence• Reliable source some of the time
D Not Usually Reliable	<ul style="list-style-type: none">• Definite doubt about authenticity, trust• Definite doubt about competence• History of occasional reliability
E Unreliable	<ul style="list-style-type: none">• Great doubt about authenticity, trust• Great doubt about competence• History of unreliable information
F No Judgment	<ul style="list-style-type: none">• Cannot be judged• No information to base decision

Information Validity

1 Confirmed	<ul style="list-style-type: none">• Confirmed by other independent sources• Logical in itself• Agrees with other information on subject
2 Probably True	<ul style="list-style-type: none">• Not confirmed• Logical in itself• Agrees with other information on subject
3 Possibly True	<ul style="list-style-type: none">• Not confirmed• Reasonably logical in itself• Agrees somewhat with other information
4 Doubtfully True	<ul style="list-style-type: none">• Not confirmed• Not illogical in itself• Not believed when received, but possible
5 Improbable Report	<ul style="list-style-type: none">• The contrary is confirmed• Is illogical in itself• Contradicted by other information
6 No Judgment	<ul style="list-style-type: none">• Cannot be judged• No information to base decision

NATIONAL INTELLIGENCE COUNCIL (NIC)

Our assessments and estimates are supported by information that varies in scope, quality, and sourcing. Consequently, we ascribe *high, moderate, or low* levels of confidence to our assessments, as follows:

High Confidence generally indicates that our judgments are based on high-quality information, and/or that the nature of the issue makes it possible to render a solid judgment. A “high confidence” judgment is not a fact or a certainty, however, and such judgments still carry a risk of being wrong.

Moderate Confidence generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.

Low Confidence generally means that the information’s credibility and/or plausibility is questionable, or that the information is too fragmented or poorly corroborated to make solid analytic inferences, or that we have significant concerns or problems with the sources.