The Cyber Shafarat - Treadstone 71

We See What Others Cannot – WWW.TREADSTONE71.COM

ADVERSARIES, ANONYMOUS, ASHIYANE, BEHAVIOR ANALYSIS, CEO, CFO, CICBK, CICMM, CIO, CISO, CLANDESTINE, COUNTERINTELLIGENCE, COUNTERSTRIKE, CYBER INTELLIGENCE, CYBER INTELLIGENCE CAPABILITY MATURITY MODEL, CYBER INTELLIGENCE CBK, CYBER INTELLIGENCE COMMON BODY OF KNOWLEDGE, CYBER OPERATIONS, CYBER PSYOPS, CYBER THREAT INTELLIGENCE, CYBER TRAINING, CYBER WARFARE, ESPIONAGE, GRU, HUMINT, HUNT, ICS, INCIDENT RESPONSE, INFORMATION SECURITY, INFOSEC, INTELLIGENCE ANALYSIS, INTELLIGENCE ESTIMATE, INTELLIGENCE TRAINING, OSINT, PLC, PROGRAMMABLE LOGIC CONTROLLER, REPORTING, RSA CONFERENCE, RUSSIA, SABOTAGE, SANS, SANSPAPER, SANSTIP, SCADA, TARGET CENTRIC, TARGET-CENTRIC, THREAT INTELLIGENCE, THREAT INTELLIGENCE TRAINING, TRADECRAFT, TREADSTONE 71 CYBER INTELLIGENCE CAPABILITY MATURITY MODEL

Dragonfly 2.0? Delta Elektroniks and Pre-embedded Malware

Date: 06/09/2017Author: Treadstone 71 ☐ 0 Comments

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

Treadstone 71 asserts with high confidence that Delta Elektroniks (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. 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)
- Multiple other sites deliver the same software (C3) …

The full report: Intelligence Games in the Power Grid – 2016

The associated PPTX: Treadstone 71 Intelligence Games in the Power Grid

Many of the original files are located here: http://ow.ly/3Ly730f2P0A

Use Hybrid-Analysis.com or https://joesecurity.org/

Recent reports from Symantec:

http://www.eweek.com/security/dragonfly-2.0-hackers-targeting-the-energy-sector-symantec-finds

https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

https://www.linkedin.com/feed/update/urn:li:activity:6312660838863945728/

Published by Treadstone 71

@Treadstone71LLC cyber intelligence, counterintelligence, infiltration, OSINT, Clandestine Cyber HUMINT, cyber intel and OSINT training and analysis, cyber psyops, strategic cyber security, Interim CISO Services View all posts by Treadstone 71