VARNOST KRITIČNE INFRASTRUKTURE

Dan informacijske varnosti
Institut Jožef Stefan, 8.11.2017

Blaž Ivanc
Attackers are getting more aggressive

• From information gathering to equipment disruption
  – BlackEnergy malware → crimeware tool (2007)
    • BE2 → modular tool (2010)
    • BE3 → focused on core functionality (2014)
  – Havex malware - remote access trojan for ICS (2014) → industrial espionage
  – Cyberattack on Ukrainian power grid (2015/2016) → BE for remote access
Sandworm (BE3)
- The use of zero-day vulnerabilities.
- European Union, NATO, energy sector.

DragonFly 2.0 (2015 → 2017)
- Motives: intelligence gathering / sabotage
- Methods: spear phishing emails / trojanized software / watering hole websites
Re: New Order P08112016 - URGENT - Daily

From: Kiril Georgiev <Kiril.Georgiev@...>

Subject: Re: New Order P08112016 - URGENT

To: info@...<br>

Greetings Sir,<br>

Hope you are fine.<br>

Please find enclosed our new order P08112016 for your kind approval and prompt execution.<br>

I look forward to receiving your order acknowledgement in due course.<br>

Best regards,<br>

Kiril Georgiev<br>Buckinghamshire Office<br>Eastern Europe<br>138 Tintyva Str., entr.1<br>1113 Sofia, Bulgaria<br>Ph. +359 2 86 86 896<br>Fax: +359 2 86 81 475<br>Mobile: +359 884 466 040<br>Kiril.Georgiev@...
Different cybercriminal groups are cooperating closely with each other

CCleaner v5.33.6162 (Floxif)

Necurs (E-mail → Ransom.Locky / Trojan.Trickybot)
  - Gathering operational intelligence
  - Downloader:
    - screen grab (PowerShell script)
    - error-reporting capability
1. Send $300 worth of Bitcoin to following address:

1Mz7153HMuXTxR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

J3mE9S-8XNTZd-ZgjYXb-fUFj8m-gMYdyv-6rEiYa-KevGjA-q8YZf4-5LP82d-ew5GUV

If you already purchased your key, please enter it below.

Key: _

• **Industroyer**
  – modular malware
    • custom tools (port scanner, DoS tool)
  – communication with the C&C servers
    • under the radar
  – payloads work in stages
  – masquerading (additional backdoor)

• **Worm-type ransomware**
  – ZCryptor
  – WannaCry
  – Petya
Cyber Attacks in Critical Infrastructure

- **Understanding the system** prior to the attack enables the attackers to implement more complex attack.

- After the attacker has broken into the critical infrastructure network, the following threats are common: *response injection*, *command injection*, and *denial of service*.

  - The known weakness of communication protocols in ICS is the **absence of the appropriate authentication**, which enables *false data injection* and *false response packets*.

  - The absence of **verifying the integrity of measurement data** in sensors enables *response injection* and consequently *inappropriate responses* in relation to the actual situation.
Cyber Attacks in Critical Infrastructure

- **Deception attacks**
  - The attacks with the goal of deception can be found in the industrial control systems as a *change in the parameter values* and can, as a result, impact on the behaviour of components, e.g. switches, controllers, and actuators.
  - Deception attacks vs. replay attacks

- **False data injection attack**
  - Attacker can *inject random or target false data*.
  - Stealth attack.
  - Identifying the network models can enable the attacker to implement simple attacks that are yet hard to detect.

- **Network traversal attack**
  - Attack penetrates the network layers and enables the attacker the path to the key elements of industrial control systems by *exploiting the trust relationship* among the network hosts.
Case Study – Cyber Attack on Critical Infrastructure
(Penetration Test and Cyber Resilience Assessment in 2013)

- Water and sewage company
  Persons authorized for the management of the water supply system

- System integrator
  Provider/operator of the monitoring centre for the management of the water supply system

- Field facilities
  (pumping stations, water storage tanks ...) Remote Terminal Unit location

- INTERNET

- GPRS/VPN
Node Description
G-0  Cyber-attacks in critical infrastructure
G-1  Reconnaissance and attack development
G-2  The attack on industrial control systems
G-3  Getting acquainted with the field data
G-4  Development of offensive computer-network operation in the mirrored environment.
G-5  Direct compromising of the industrial control systems
G-6  Attack on the system integrator level
G-7  Acquiring documentation and program files
G-8  Computer network analyses
G-9  Attacks on a field level
G-10 Exploiting the weakness of routine procedures
G-11 Embedding backdoor in IT systems
G-12 Data manipulation
G-13 Capturing data flow traffic
G-14 Data flow emission
G-15 Traffic processing
G-16 Program change in programmable logic controller
G-17 Manipulation on sensor level
G-18 Compromising communication paths
G-19 Remote manipulation through additional users
G-20 Local manipulation of the process database
G-21 Adding communication paths
G-22 Embedding of the MitM attack mechanism
The **target** can often be the **system integrator** of the industrial control system in the critical infrastructure. This raises the following questions:

- Can the operator of the critical infrastructure prevent concrete information attacks that exploit the system integrator as an entry point?
- Can the operator of the critical infrastructure prevent a security incident resulting from compromising technology on the level of the manufacturer?
- Has the operator of the critical infrastructure considered information attacks originating from compromising higher structures (systems integrator, technology producer) while performing risk assessment and was the operator able to provide concrete security countermeasures?

System **supply chain** is the appropriate **point** for **compromising**, especially in terms of structures that can represent more demanding attack techniques or merely exploit its situation in the required access to the application with simple offensive methods.
Cyber Attacks in Critical Infrastructure

- **Key features of novel cyber-attacks**
  - The attacks are focused on **compromising data integrity** with the aim of causing consequences in the physical space
  - The attacks reveal **new offensive information techniques**
  - The malicious code **dropper** can **exploit** at least one of the **unknown software vulnerabilities** with the purpose of expanding or raising the privileges
  - Autonomous generating of the system specific payload
Critical infrastructure operators are advised to establish cyber defense departments which will review security issues in terms of threat agents.

Sophisticated critical infrastructure attack analyses show that attacks executing a discrete covert channel are a relatively evenly distributed combination of a physical and a cyber attack supported by extensive intelligence efforts.

According to the findings more security measures should be introduced in Slovenia immediately:

- Mandatory introduction and monitoring of the implementation of security standards for industrial control systems.
- It is necessary to determine the level of independence of the critical infrastructure operator in terms of physical process management through industrial-control systems.
- It would be wise to establish a small, highly competent organization for cyber security and CIP. In Slovenia, this would ensure a secure supply of individual system components, assessment of adequate security mechanisms, forcing the local know-how to pursue constant development and monitor the progress of technology related areas.
INFOSEC Aspects of the Europe-wide Public Safety Data Interoperability Network

- **Challenges**
  - interoperability
  - broadband connectivity
  - lack of coverage
  - destroyed infrastructure
  - technological gaps with commercial technologies

- Communication in the public safety agencies is slowly shifting from predominantly audio messages to *media enriched broadband communication*
  - *At the time of emergency response*: sensitive voice information, videos, images, maps, data from different records ...
INFOSEC Aspects of the Europe-wide Public Safety Data Interoperability Network

- Security requirements of the system
  - It is necessary for agencies to have the ability to decide what resources should be shared or disclosed to their partners at any given moment.
  - Communication with and within the system must be secured and encrypted.
  - Even if the information is not classified (such as EU Sensitive) it cannot be transmitted over unprotected channels in plain text form.
  - Storage of all the data gathered by agencies should be encrypted and protected.
The range of approaches to address the security aspects

- Security risks have been identified for each key component of the system already during the design.

- The implemented security mechanisms and good practices correspond to the proposed risk mitigation strategies.

- During security guidance, monitoring and system evaluation, we used a number of operational and technically specific approaches.
Node Description

G-0 System component attack
G-1 WAN-based attacks
G-2 Local network attacks on end-user
G-3 Implementation attacks
G-4 Infrastructure attacks
G-5 Direct local access
G-6 Man-in-the-Middle implementations
G-7 Other unclassified implementations
G-8 SQL injections
G-9 Brute-force approaches
G-10 DoS/DDos attacks
G-11 Client side attacks
G-12 Tautologies
G-13 Piggy-backed queries
G-14 Stored procedures
G-15 Inference and alternate encodings
G-16 DNS amplification attack
G-17 ICMP flood attack
G-18 TCP SYN flood denial-of-service attack
G-19 Spear phishing
G-20 Watering-hole attack
G-21 Prompt user to enable macros
G-22 Drop malicious .vbs file
G-23 Trojan installation
G-24 Redirection of visitors to a malicious server
G-25 Fingerprinting script execution
G-26 Configuration information extraction
G-27 Installation attempt of a trojanized version of the software
P-1 Dropping the set of trojans
O-1 Dictionary attacks
INFOSEC Aspects of the Europe-wide Public Safety Data Interoperability Network

- Security overview of system components and security assessments
  - Overview of security mechanism for individual system component
    - Platform (➔)
    - Main Switch
    - Core Data Storage
    - Ontology Services
    - Collaboration Web
    - Open-source Gateway
    - Plug-in(s)

  - Firewall
    - The use of [redacted] All ports that are not in use by the running services are blocked. Two separate scripts for normal operations and lockdown [redacted]. Furthermore, three unsuccessful login attempts disable the user from login for 600 seconds.

  - Trusted Certificate
    - Trusted certificate chain is installed. All services accessed by [redacted] users are configured to use it.

  - MySQL user accounts management
    - Each service that needs to utilize database for its correct functionality, has its own account, to reduce the possibility of collateral data damage.

  - Mail service secure access
    - [redacted] (SMTP server) and [redacted] (IMAP server) configured to accept only [redacted] communication.

  - Mail service anti-virus and anti-spam protection
    - [redacted] installed and configured.
Safe design and implementation (features below) [R04]

- 3-tier application
- Validation of all input
- SQL injection protection
- XSS protection
- Server Side Include Injection
- Replay attack protection
- CSRF protection
- Command injection protection
- LDAP injection protection
- XPath injection protection
- Resource injection protection
- Log injection protection
- XML poisoning
- Session hijacking protection
- Automatic session log-out
- Cookies protection
- No stored password for access to resource (connection strings, etc.)
- Character set is specified in every page
- No technical data leakage
- No internal error messages, like stack trace, etc.
- Buffer overflow

[Collaboration Web, Core Data Storage, Gateway, Ontology, Secure Agent Infrastructure, Monitor Centre]
Incident Response

- Collect data
- Stop malware propagation
- Identify and analyze threat
- Find all affected machines
- Forensics at first affected system
- Mitigation & Reporting
Scenario-Based {Planning, Learning, ...}
Ensuring cyber security is a **dynamic, demanding, and complex** task.

- Build the right **team** and structure
- Prepare **concrete** policies, procedures, standards, and guidelines
- **Integrate** a cyber intelligence support
- **Recognize** and defend single point of failure parts
- Have an **understanding** of security operations concepts.

Cyber security experts are forced to engage in constant **education**, having **access to test environments** and develop both **offensive** and **defensive** information techniques.
Vprašanja ...

blaz.ivanc@determinanta.si