THREAT INTELLIGENCE REPORT

EXAMPLE NETWORK 001

20 Feb - 27 Feb 2019

DARKTRACE
INDUSTRIAL

THREAT INDICATOR KEY

Board Advisory
Darktrace advises that immediate consultation with the Chief Executive and Board is considered

Any incident (ongoing or detected) that has the potential for severe commercial, legal and or operational impact. For example, large scale or unexplained data loss; inability to exercise operational control; any activity that denies critical mission delivery; significant data integrity or core service accessibility issues.

General Counsel Advisory
Darktrace advises that the General Counsel be briefed immediately

Any incident (ongoing or detected) that could expose the organization to legal challenge; the GC at his or her discretion may wish to appraise the Executive team. For example, the use of the IT estate for malicious purposes (botnet or malware hosting and/or delivery); compromised corporate services used as a staging post or attack vector against a third party.

Enhanced Caution Advised
Darktrace advises that the incident is of sufficient gravity that it should have further internal forensic investigation

Any incident (ongoing or detected) that could indicate a risk to the organization if not addressed. There are indicators of probable compromise such as active command and control communications, etc. Security staff should be aware of the issue and action taken ASAP.

Security Policy Advisory
Darktrace advises that the organization's security and compliance function consider incorporating the finding into policy

Any incident (ongoing or detected) that has the potential to be a risk to the organization through failure to comply with organizational policies, such as BYOD compliance; bad security practice (sharing of passwords or accounts); data risk (uploading to third party data repositories outside of the corporate network), etc.

EXECUTIVE SUMMARY

Darktrace has been successfully installed and has begun its learning process. This learning will continue to become richer and richer throughout the Proof of Value. For increased security, Darktrace's team will only refer to the customer using a codename. This is the first Threat Intelligence Report prepared by Darktrace, highlighting three incidents this week for further investigation:

Darktrace has detected unusual communications between company employees at head offices in London and Edinburgh, and devices within ICS networks. A corporate user remotely controlled an ICS device at an unusual time (outside working hours) and likely instructed it to pass backup and network management files into the corporate network. This may be an unauthorized acquisition of sensitive data that would give critical clues as to the functioning of the ICS network and potential points of entry and vulnerability. Other unusual and successful connections between the corporate and ICS networks have also been observed and we would recommend confirming that the networks and relevant firewalls have been set up as intended.

EXECUTIVE SUMMARY

Darktrace detected an unknown command being accepted by an ICS control device; acceptance of the command may indicate there is an engineering backdoor allowing access to the device with unknown capabilities. Subsequently Darktrace detected a change in the device's behavior as it began responding differently to regular command messages. The device appears to have been reprogrammed, suggesting that an attacker may be actively exploiting the security flaw to cause it to malfunction.

A number of ICS devices this week began sporadically broadcasting system information to other devices on the network. This represented a departure from their usual behavior, as such extensive broadcasts have been modeled as rare. Such activity may provide additional information to attackers and the company may wish to restrict these behaviors if they are not part of a necessary business process.

A laptop on the company's enterprise network has made numerous anomalous connections to core ICS control devices. The connections – many of which failed – appear to constitute an effort to identify key ICS devices and test their connectivity and potential vulnerabilities. Communication between this laptop and the ICS network is unprecedented and should be investigated as a case of malicious reconnaissance.

INCIDENT 1

Connections from Corporate Network

A device on the corporate network was detected controlling a device within an ICS network via SSH at an unusual time. Shortly afterwards data was sent back to the corporate device over FTP. Typically this ICS network device makes outbound connections to other machines in the ICS network but very rarely receives connections.

172.16.1.0 (within the London Head Office corporate subnet) connected to **192.168.1.0** (within the ICS configuration subnet) on TCP port 22 (SSH). SSH connections at this time (outside of working hours) have so far been modeled as anomalous.

The next day, **192.168.1.0** failed to connect to **172.16.1.0** on TCP port 20 (FTP DATA). A successful connection followed:

192.168.1.0 connected to **172.16.1.0** on TCP port 2624 (passive FTP data) and transferred a number of files to the corporate device. Darktrace detected this as 81% unusual as data transfer between devices in these subnets (i.e. between the corporate and ICS networks) is unusual.

Among the transferred files were the following:

- Backup.zip
- Configurationplans.zip
- Briefings.zip

- Prior to this **10.24.40.59** and **10.24.40.219** (Edinburgh office) both made SMB connections to **192.168.2.1** (ICS subnet workstation running Windows 7) within one second of each other, beginning at 10:34. The devices authenticated with username ‘admin’ and proceeded to make the Remote Procedure Call ‘NetWkstaEnumUsers’, requesting user enumeration of the ICS subnet workstation.

INCIDENT 2

Compromise Behaviors

A PLC was observed receiving and accepting an unknown Modbus function code. This command has not been seen before on this network. It may indicate the use of a backdoor into the device.

192.168.3.2 connected to **192.168.3.108:501** using MODBUS Function Code 0x5A. A non-exception response was returned indicating that the commands were accepted by this PLC device.

192.168.3.2 made three requests for **192.168.3.108:501** using MODBUS Function Code 0x5A. Non--exception responses were received indicating that the commands were accepted. Use of this function code had not been seen before and is highly unusual on the network, and no other occurrences have been observed since. No other changes in the behavior of the PLC device were seen.

Function Code 0x5A is not a standard MODBUS function code and its capabilities are unknown. Its use may have been triggered by an operator, or by an unusual condition within the automated control system. It did not obviously affect the integrity of the receiving PLC, but could be reconnaissance either retrieving data or confirming that the command can be used successfully.

We recommend that this is investigated further. The process historian may provide useful information on how the command was triggered and why. The PLC documentation should be reviewed for the nature of Function Code 0x5A, if this is not already known by the network operators. If necessary, the PLC manufacturer should be consulted.

INCIDENT 3

Devices Broadcasting System Information

Several ICS devices broadcast system information to their entire local network. The spontaneous nature of this broadcast activity may be of concern as the devices could easily be identified by a would-be attacker.

Between Wed 11:52:01 and 11:53:42 several ICS devices broadcast system metrics on UDP ports 51338, 51339, 51342, 51344 and 51346 to the broadcast address 255.255.255.255:

• **Andahl Process CENT-HMI 192.168.2.5** Andahl Process;;MAC=A0:12:84:d1:42:b4;;IP=192.168.4.195;;MASK=255.255.255.0;;GATEWAY=0.0.0.0 ;;DHCP=OFF;;FAMIL Y=CENT-HMI;;TYP=M2017007 1672;;NAME=MSPG;;SERIEN_NR=5B114A;;

• **CENT Tora RotoScrew 2H · 192.168.2.6** Andahl Process;;CLASS=200;;MAC=A0:1b:84:8d:22:cf;;IP=192.168.4.194;;MASK=255.255.255.0;;GATE WAY=0.0.0.0;;DHCP= OFF;;FAMILY=CENT Tora;;TYP=S2017001 0214;;NAME=CENT Tora WindScrew 2H;; SERIEN_NR=E450675;;

• **CENT U2 Line B Vessel 2 · 192.168.2.7** Andahl Process;;CLASS=200;;MAC=A0:1b:2d:80:ba:0c;;IP=192.168.4.203;;MASK=255.255.255.0;;GATE WAY=0.0.0.0;;DHCP =OFF;;FAMILY=CENT Tora;;TYP=W2017010 0223;;NAME=CENT T2 Vessel 3;;SERIEN_NR=EI21311;;

The following devices were announcing their existence at this time:

192.168.2.80, 192.168.2.81, 192.168.2.82, 192.168.2.83, 192.168.2.84, 192.168.2.85

INCIDENT 4

ICS Reconnaissance from Enterprise Device

The device was initially detected making a new failed TCP connection to a PLC on port 2222 (cip_explicit_tcp), which was rejected. Further investigation revealed that the laptop made a VNC connection to an HMI a few minutes before, although this only lasted for eleven seconds. The laptop was also detected making an ICS discovery request to a PLC device, which appears to have responded. Several attempts were made to connect to other PLCs on various subnets, however none of these were successful.

Connection 1
Time: Thursday 23:55:35
Source: inthqeast 198.233.73.67
Destination: 10.34.56.126
Port: 2222
Status: Failed (SYN – RST)

Connection 2
Time: Thursday 23:53:23 – 23:53:34
Source: inthqeast 198.233.73.67
Destination: 10.233.56.34
Port: 5900
Status: SYN-ACK-SYN-ACK

Connection 3
Time: Thursday 23:54:45
Source: inthqeast 198.233.73.67
Destination: 10.34.56.233, 10.16.56.126, 10.255
PCAP: nmap -sP --script s7-discover.nse -p 102 <host/s>