The Trojan Horse Malware & Password “Cracking” Ecosystem Targeting Industrial Operators

By Sam Hanson

Published: 2022-07-14 · Archived: 2026-04-10 02:10:21 UTC

The internet brings endless possibilities for scammers and cyber criminals to make money illegitimately. The usual suspects – ransomware, business email compromise, internet fraud, and phishing are well known to the information security community. However, during a routine vulnerability assessment, Dragos researchers uncovered a smaller in scale technique targeting industrial engineers and operators.

The Story of Troy and the Password “Cracking” Trojan Horse

Multiple accounts across a variety of social media websites are advertising Programmable Logic Controller (PLC), Human-Machine Interface (HMI), and project file password cracking software. Buyers can retrieve forgotten passwords by running an executable provided by the seller that targets a specific industrial system.

An advertisement like this raises the question, “Who would buy this?” Any information security professional would caution against downloading and running software from an untrusted party. Take the following as an example: an engineer named Troy just got promoted to senior engineer when his old colleague, Hector, retired after serving 30 years at an electric utility. Troy needs to update some ladder logic Hector wrote on Automation Direct’s DirectLogic 06 PLC. After firing up the PLC programming software, DirectSOFT, a password prompt pops up.

Troy doesn’t know the password, and Hector left a few months ago and is now vacationing on a boat without service indefinitely. Troy looks for answers online, and seeing an advertisement for PLC password cracking software, decides to give it a go. Cassandra, Troy’s security-conscience coworker, warns against introducing this unnecessary risk into their OT environment. But Troy insists this is a time-sensitive task. He purchases the software and runs it on his engineering workstation.

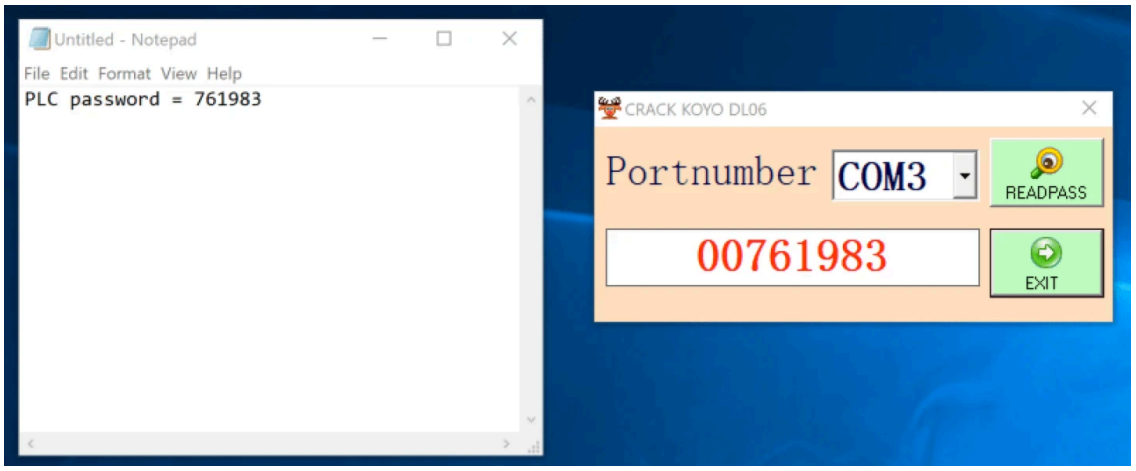
Troy successfully recovers the PLC password, but a couple of minutes later he discovers the engineering workstation system is acting strange.

Password Retrieval and a Sality Malware Infection

Troy called in Dragos to reverse engineer the password “cracking” software and determined it did not crack the password at all, rather, it exploited a vulnerability in the firmware which allowed it to retrieve the password on command. Further, the software was a malware dropper, infecting the machine with the Sality malware and turning the host into a peer in Sality’s peer-to-peer botnet.

The Exploit

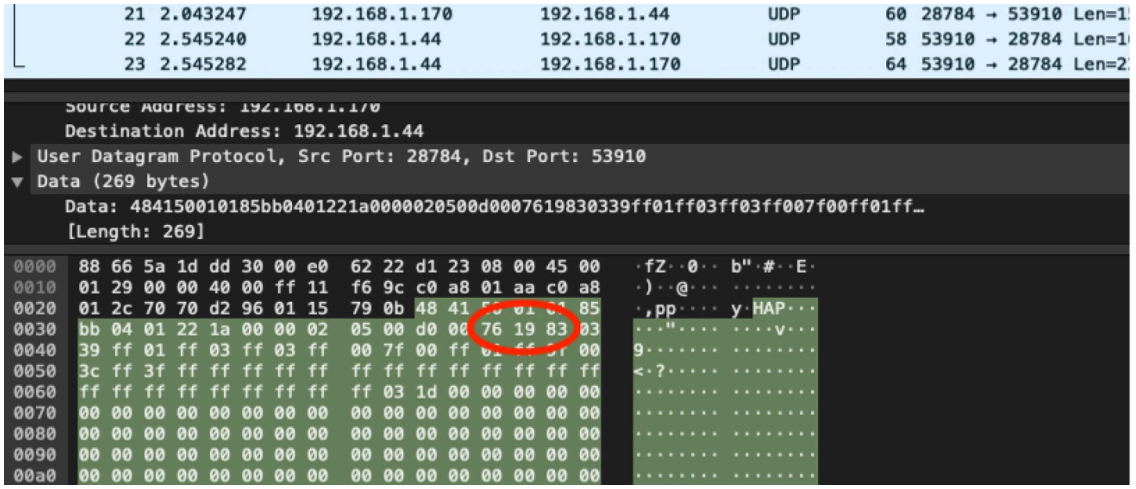
Dragos researchers confirmed the password retrieval exploit embedded in the malware dropper successfully recovers Automation Direct's DirectLogic 06 PLC password over a serial connection. From a user's perspective, they simply need to have a connection from the Windows machine to the PLC, then specify the COM port to communicate over and click the "READPASS" button. A second or two later, the password is shown to the user as seen in Figure 1.



Previous research targeting DirectLogic PLCs has resulted in successful cracking techniques. However, Dragos found that this exploit does not crack a scrambled version of the password as historically seen in popular exploitation frameworks. Instead, a specific byte sequence is sent by the malware dropper to a COM port.

IRP_MJ_READ	DOWN		
IRP_MJ_READ	UP	STATUS_SUCCESS	4b 21 06 06 02 05 00 d0 00 76 19 83 03 39

Capturing the serial traffic sent by the exploit allowed Dragos researchers to recreate it outside of the malware dropper. The malware contains a serial-only version of the exploit, requiring the user to have a direct serial connection from an Engineering Workstation (EWS) to the PLC. Dragos researchers were able to successfully recreate the exploit over Ethernet, increasing the severity of this vulnerability significantly. This vulnerability was assigned CVE-2022-2003 and was responsibly disclosed to Automation Direct. They have released a firmware update to fix this issue [source: ICS-CERT Advisory (ICSA-22-167-03), ICS-CERT Advisory (ICSA-22-167-02)].



The Sality Malware

Sality is a peer-to-peer botnet for distributed computing tasks such as password cracking and cryptocurrency mining. A Sality infection could risk remote access to an EWS by an unknown adversary. Dragos assesses with moderate confidence the adversary, while having the capability to disrupt industrial processes, has financial motivation and may not directly impact Operational Technology (OT) processes.

Sality employs process injection and file infection to maintain persistence on the host. It abuses Window's autorun functionality to spread copies of itself over Universal Serial Bus (USB), network shares, and external storage drives. This specific sample of Sality also drops clipboard hijacking malware that, every half second, checks the clipboard for a cryptocurrency address format. If seen, the hijacker replaces the address with one owned by the threat actor. This in-real-time hijacking is an effective way to steal cryptocurrency from users wanting to transfer funds and increases our confidence that the adversary is financially motivated.

To remain undetected, Sality drops a kernel driver and starts a service to identify any potential security products such as antivirus systems or firewalls and terminates them. According to various reports online, Sality is able to conduct Internet Protocol (IP) filtering against antivirus-related URLs and will drop any outgoing packets containing specific keywords known to be connected to antivirus vendor websites. This could have regulatory implications – since Sality blocks any outgoing connections, antivirus systems will not be able to receive updates violating reliability standard CIP-007-6. While Sality makes several attempts to stay hidden, it is quite clear that an infection is taking place. Central Processing Unit (CPU) levels spikes to 100% and multiple Windows Defender alerts were triggered.

Automation Direct is far from the only vendor affected. In fact, Dragos is aware that this specific threat actor advertises "cracking" software for several PLCs, HMIs, and project files listed in the following table:

Vendor and Asset	**System Type**
Automation Direct DirectLogic 06	PLC
Omron CP1H	PLC
Omron C200HX	PLC
Omron C200H	PLC
Omron CPM2*	PLC
Omron CPM1A	PLC
Omron CQM1H	PLC
Siemens S7-200	PLC
Siemens S7-200	Project File (*.mwp)
Siemens LOGO! 0AB6	PLC
ABB Codesys	Project File (*.pro)

Delta Automation DVP, ES, EX, SS2, EC Series	PLC
Fuji Electric POD UG	HMI
Fuji Electric Hakko	HMI
Mitsubishi Electric FX Series (3U and 3G)	PLC
Mitsubishi Electric Q02 Series	PLC
Mitsubishi Electric GT 1020 Series	HMI
Mitsubishi Electric GOT F930	HMI
Mitsubishi Electric GOT F940	HMI
Mitsubishi Electric GOT 1055	HMI
Pro-Face GP Pro-Face	HMI
Pro-Face GP	Project File (*.prw)
Vigor VB	PLC
Vigor VH	PLC
Weintek	HMI
Allen Bradley MicroLogix 1000	PLC
Panasonic NAIS F P0	PLC
Fatek FBe and FBs Series	PLC
IDEC Corporation HG2S-FF	HMI
LG K80S	PLC
LG K120S	PLC
Vendor and Asset	**System Type**
Automation Direct DirectLogic 06	PLC
Omron CP1H	PLC
Omron C200HX	PLC
Omron C200H	PLC
Omron CPM2*	PLC
Omron CPM1A	PLC

Omron CQM1H	PLC
Siemens S7-200	PLC
Siemens S7-200	Project File (*.mwp)
Siemens LOGO! 0AB6	PLC
ABB Codesys	Project File (*.pro)
Delta Automation DVP, ES, EX, SS2, EC Series	PLC
Fuji Electric POD UG	HMI
Fuji Electric Hakko	HMI
Mitsubishi Electric FX Series (3U and 3G)	PLC
Mitsubishi Electric Q02 Series	PLC
Mitsubishi Electric GT 1020 Series	HMI
Mitsubishi Electric GOT F930	HMI
Mitsubishi Electric GOT F940	HMI
Mitsubishi Electric GOT 1055	HMI
Pro-Face GP Pro-Face	HMI
Pro-Face GP	Project File (*.prw)
Vigor VB	PLC
Vigor VH	PLC
Weintek	HMI
Allen Bradley MicroLogix 1000	PLC
Panasonic NAIS F P0	PLC
Fatek FBe and FBs Series	PLC
IDEC Corporation HG2S-FF	HMI
LG K80S	PLC
LG K120S	PLC

Dragos only tested the DirectLogic-targeting malware. However, initial dynamic analysis of a couple of other samples indicate they also contain malware. In general, it appears there is an ecosystem for this type of software.

Several websites and multiple social media accounts exist all touting their password “crackers.”

Mitsubishi FX3U Password Crack Free Download

2022-05-09

Mitsubishi FX3G FX3G-14MR/ES, FX3G-14MT/ES, FX3G-14MT/ESS, FX3G-14MR/DS FX3G-14MT/DS

37

Read More

Unlock PLC Mitsubishi FX3G FX3GA Free Download 100% Working

2022-05-01

FX3G-14MR/ES, FX3G-14MT/ES, FX3G-14MT/ESS, FX3G-14MR/DS FX3G-14MT/DS, FX3G-14MT/DSS,

37

Read More

Conclusion

Trojanized software is a common delivery technique for malware and has been proven effective for gaining initial access to a network. While, in our fictitious example, Troy had a legitimate reason for downloading the password "cracking" software, doing so from an unknown actor introduced significant and unnecessary risk into the OT environment. If an engineer needs to recover a lost password, contact Dragos or the respective vendor for instructions and guidance. As the adage goes, if it's too good to be true, then it probably is.

Sam Hanson is a Vulnerability Analyst on the Intelligence Research Team. Sam graduated from the University of Minnesota – Twin Cities in 2020 with a Computer Science degree and a focus on Computer Security.
