Last 5 Pages Viewed: Exploitation of Remote Services » Drive-by Compromise » ATT&CK® for Industrial Co... » Initial Access

Initial Access

Description

The adversary is trying to get into your ICS environment.

Initial Access consists of techniques that adversaries may use as entry vectors to gain an initial foothold within an ICS environment. These techniques include compromising operational technology assets, IT resources in the OT network, and external remote services and websites. They may also target third party entities and users with privileged access. In particular, these initial access footholds may include devices and communication mechanisms with access to and privileges in both the IT and OT environments. IT resources in the OT environment are also potentially vulnerable to the same attacks as enterprise IT systems. Trusted third parties of concern may include vendors, maintenance personnel, engineers, external integrators, and other outside entities involved in expected ICS operations. Vendor maintained assets may include physical devices, software, and operational equipment. Initial access techniques may also leverage outside devices, such as radios, controllers, or removable media, to remotely interfere with and possibly infect OT operations.

Techniques in this Tactics Category

Below is a list of all the Initial Access techniques in ATT&CK for ICS:

Name	Tactics	Technical Description
Drive-by Compromise	Initial Access	Adversaries may gain access to a system during a drive-by compromise, when a user visits a website as part of a regular browsing session.With this technique, the user's web browser is targeted and exploited simply by visiting the compromised website. The adversary may target a specific community, such as trusted third party suppliers or other industry specific groups, which often visit the target website. This kind of targeted attack relies on a common interest, and is known as a strategic web compromise or watering hole attack. The National Cyber Awareness System (NCAS) has issued a Technical Alert (TA) regarding Russian government cyber activity targeting critical infrastructure sectors.[1] Analysis by DHS and FBI has noted two distinct categories of victims in the Dragonfly campaign on the Western energy sector: staging and intended targets. The adversary targeted the less secure networks of staging targets, including trusted third-party suppliers and related peripheral organizations. Initial access to the intended targets used watering hole attacks to target process control, ICS, and critical infrastructure related trade publications and informational websites.
Exploit Public-Facing Application	Initial Access	Adversaries may leverage weaknesses to exploit internet-facing software for initial access into an industrial network. Internet-facing software may be user applications, underlying networking implementations, an assets operating system, weak defenses, etc. Targets of this technique may be intentionally exposed for the purpose of remote management and visibility. An adversary may seek to target public-facing applications as they may provide direct access into an ICS environment or the ability to move into the ICS network. Publicly exposed applications may be found through online tools that scan the internet for open ports and services. Version numbers for the exposed application may provide adversaries an ability to target specific known vulnerabilities. Exposed control protocol or remote access ports found in Commonly Used Port may be of interest by adversaries.
Exploitation of Remote Services	Lateral Movement Initial Access	Adversaries may exploit a software vulnerability to take advantage of a programming error in a program, service, or within the operating system software or kernel itself to enable remote service abuse. A common goal for post-compromise exploitation of remote services is for initial access into and lateral movement throughout the ICS environment to enable access to targeted systems.[2] ICS asset owners and operators have been affected by ransomware (or disruptive malware masquerading as ransomware) migrating from enterprise IT to ICS environments: WannaCry, NotPetya, and BadRabbit. In each of these cases, self-propagating (“wormable”) malware initially infected IT networks, but through exploit (particularly the SMBv1-targeting MS17-010 vulnerability) spread to industrial networks, producing significant impacts.[3]

Name	Tactics	Technical Description
External Remote Services	Initial Access	Adversaries may leverage external remote services as a point of initial access into your network. These services allow users to connect to internal network resources from external locations. Examples are VPNs, Citrix, and other access mechanisms. Remote service gateways often manage connections and credential authentication for these services.[4] External remote services allow administration of a control system from outside the system. Often, vendors and internal engineering groups have access to external remote services to control system networks via the corporate network. In some cases, this access is enabled directly from the internet. While remote access enables ease of maintenance when a control system is in a remote area, compromise of remote access solutions is a liability. The adversary may use these services to gain access to and execute attacks against a control system network. Access to valid accounts is often a requirement. As they look for an entry point into the control system network, adversaries may begin searching for existing point-to-point VPN implementations at trusted third party networks or through remote support employee connections where split tunneling is enabled.[5] In the Maroochy Attack, the adversary was able to gain remote computer access to the system over radio.
Internet Accessible Device	Initial Access	Adversaries may gain access into industrial environments through systems exposed directly to the internet for remote access rather than through External Remote Services. Internet Accessible Devices are exposed to the internet unintentionally or intentionally without adequate protections. This may allow for adversaries to move directly into the control system network. Access onto these devices is accomplished without the use of exploits, these would be represented within the Exploit Public-Facing Application technique. Adversaries may leverage built in functions for remote access which may not be protected or utilize minimal legacy protections that may be targeted.[6] These services may be discoverable through the use of online scanning tools. In the case of the Bowman dam incident, adversaries leveraged access to the dam control network through a cellular modem. Access to the device was protected by password authentication, although the application was vulnerable to brute forcing.[6][7][8] In Trend Micro’s manufacturing deception operations adversaries were detected leveraging direct internet access to an ICS environment through the exposure of operational protocols such as Siemens S7, Omron FINS, and EtherNet/IP, in addition to misconfigured VNC access.[9]

Name	Tactics	Technical Description
Remote Services	Lateral Movement Initial Access	Adversaries may leverage remote services to move between assets and network segments. These services are often used to allow operators to interact with systems remotely within the network, some examples are RDP, SMB, SSH, and other similar mechanisms.[10][11][3] Remote services could be used to support remote access, data transmission, authentication, name resolution, and other remote functions. Further, remote services may be necessary to allow operators and administrators to configure systems within the network from their engineering or management workstations. An adversary may use this technique to access devices which may be dual-homed[10] to multiple network segments, and can be used for Program Download or to execute attacks on control devices directly through Valid Accounts. Specific remote services (RDP & VNC) may be a precursor to enable Graphical User Interface execution on devices such as HMIs or engineering workstation software. In the Oldsmar water treatment attack, adversaries gained access to the system through remote access software, allowing for the use of the standard operator HMI interface.[12] Based on incident data, CISA and FBI assessed that Chinese state-sponsored actors also compromised various authorized remote access channels, including systems designed to transfer data and/or allow access between corporate and ICS networks. [13]
Replication Through Removable Media	Initial Access	Adversaries may move onto systems, such as those separated from the enterprise network, by copying malware to removable media which is inserted into the control systems environment. The adversary may rely on unknowing trusted third parties, such as suppliers or contractors with access privileges, to introduce the removable media. This technique enables initial access to target devices that never connect to untrusted networks, but are physically accessible. Operators of the German nuclear power plant, Gundremmingen, discovered malware on a facility computer not connected to the internet.[14][15] The malware included Conficker and W32.Ramnit, which were also found on eighteen removable disk drives in the facility.[16][17][18][19][20][21] The plant has since checked for infection and cleaned up more than 1,000 computers.[22] An ESET researcher commented that internet disconnection does not guarantee system safety from infection or payload execution.[23]

Name	Tactics	Technical Description
Rogue Master	Initial Access	Adversaries may setup a rogue master to leverage control server functions to communicate with outstations. A rogue master can be used to send legitimate control messages to other control system devices, affecting processes in unintended ways. It may also be used to disrupt network communications by capturing and receiving the network traffic meant for the actual master. Impersonating a master may also allow an adversary to avoid detection. In the Maroochy Attack, Vitek Boden falsified network addresses in order to send false data and instructions to pumping stations.[24] In the case of the 2017 Dallas Siren incident, adversaries used a rogue master to send command messages to the 156 distributed sirens across the city, either through a single rogue transmitter with a strong signal, or using many distributed repeaters.[25][26]
Spearphishing Attachment	Initial Access	Adversaries may use a spearphishing attachment, a variant of spearphishing, as a form of a social engineering attack against specific targets. Spearphishing attachments are different from other forms of spearphishing in that they employ malware attached to an email. All forms of spearphishing are electronically delivered and target a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution and access.[27] A Chinese spearphishing campaign running from December 9, 2011 through February 29, 2012, targeted ONG organizations and their employees. The emails were constructed with a high level of sophistication to convince employees to open the malicious file attachments.[13]

Name	Tactics	Technical Description
Supply Chain Compromise	Initial Access	Adversaries may perform supply chain compromise to gain control systems environment access by means of infected products, software, and workflows. Supply chain compromise is the manipulation of products, such as devices or software, or their delivery mechanisms before receipt by the end consumer. Adversary compromise of these products and mechanisms is done for the goal of data or system compromise, once infected products are introduced to the target environment. Supply chain compromise can occur at all stages of the supply chain, from manipulation of development tools and environments to manipulation of developed products and tools distribution mechanisms. This may involve the compromise and replacement of legitimate software and patches, such as on third party or vendor websites. Targeting of supply chain compromise can be done in attempts to infiltrate the environments of a specific audience. In control systems environments with assets in both the IT and OT networks, it is possible a supply chain compromise affecting the IT environment could enable further access to the OT environment. Counterfeit devices may be introduced to the global supply chain posing safety and cyber risks to asset owners and operators. These devices may not meet the safety, engineering and manufacturing requirements of regulatory bodies but may feature tagging indicating conformance with industry standards. Due to the lack of adherence to standards and overall lesser quality, the counterfeit products may pose a serious safety and operational risk.[28] Yokogawa identified instances in which their customers received counterfeit differential pressure transmitters using the Yokogawa logo. The counterfeit transmitters were nearly indistinguishable with a semblance of functionality and interface that mimics the genuine product.[28] F-Secure Labs analyzed the approach the adversary used to compromise victim systems with Havex.[29] The adversary planted trojanized software installers available on legitimate ICS/SCADA vendor websites. After being downloaded, this software infected the host computer with a Remote Access Trojan (RAT).

Name	Tactics	Technical Description
Transient Cyber Asset	Initial Access	Adversaries may target devices that are transient across ICS networks and external networks. Normally, transient assets are brought into an environment by authorized personnel and do not remain in that environment on a permanent basis.[30] Transient assets are commonly needed to support management functions and may be more common in systems where a remotely managed asset is not feasible, external connections for remote access do not exist, or 3rd party contractor/vendor access is required. Adversaries may take advantage of transient assets in different ways. For instance, adversaries may target a transient asset when it is connected to an external network and then leverage its trusted access in another environment to launch an attack. They may also take advantage of installed applications and libraries that are used by legitimate end-users to interact with control system devices. Transient assets, in some cases, may not be deployed with a secure configuration leading to weaknesses that could allow an adversary to propagate malicious executable code, e.g., the transient asset may be infected by malware and when connected to an ICS environment the malware propagates onto other systems. In the Maroochy attack, the adversary utilized a computer, possibly stolen, with proprietary engineering software to communicate with a wastewater system.[24]
Wireless Compromise	Initial Access	Adversaries may perform wireless compromise as a method of gaining communications and unauthorized access to a wireless network. Access to a wireless network may be gained through the compromise of a wireless device.[31][32] Adversaries may also utilize radios and other wireless communication devices on the same frequency as the wireless network. Wireless compromise can be done as an initial access vector from a remote distance. A joint case study on the Maroochy Shire Water Services event examined the attack from a cyber security perspective.[24] The adversary disrupted Maroochy Shire's radio-controlled sewage system by driving around with stolen radio equipment and issuing commands with them. Boden used a two-way radio to communicate with and set the frequencies of Maroochy Shire's repeater stations. A Polish student used a modified TV remote controller to gain access to and control over the Lodz city tram system in Poland.[33][34] The remote controller device allowed the student to interface with the tram’s network to modify track settings and override operator control. The adversary may have accomplished this by aligning the controller to the frequency and amplitude of IR control protocol signals.[35] The controller then enabled initial access to the network, allowing the capture and replay of tram signals.[33]

References

1. ^ Cybersecurity & Infrastructure Security Agency. (2018, March 15). Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved October 11, 2019. (https://us-cert.cisa.gov/ncas/alerts/TA18-074A)
2. ^ Enterprise ATT&CK. (n.d.). Exploitation of Remote Services. Retrieved October 27, 2019. (https://attack.mitre.org/techniques/T1210/)
3. a b Joe Slowik. (2019, April 10). Implications of IT Ransomware for ICS Environments. Retrieved October 27, 2019. (https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/)
4. ^ Daniel Oakley, Travis Smith, Tripwire. (n.d.). Retrieved May 30, 2018. (https://attack.mitre.org/wiki/Technique/T1133)
5. ^ Electricity Information Sharing and Analysis Center; SANS Industrial Control Systems. (2016, March 18). Analysis of the Cyber Attack on the Ukranian Power Grid: Defense Use Case. Retrieved March 27, 2018. (https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt6a77276749b76a40/607f235992f0063e5c070fff/E-ISAC_SANS_Ukraine_DUC_5%5b73%5d.pdf)
6. a b NCCIC. (2014, January 1). Internet Accessible Control Systems At Risk. Retrieved November 7, 2019. (https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jan-April2014.pdf)
7. ^ Danny Yadron. (2015, December 20). Iranian Hackers Infiltrated New York Dam in 2013. Retrieved November 7, 2019. (https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559)
8. ^ Mark Thompson. (2016, March 24). Iranian Cyber Attack on New York Dam Shows Future of War. Retrieved November 7, 2019. (https://time.com/4270728/iran-cyber-attack-dam-fbi/)
9. ^ Stephen Hilt, Federico Maggi, Charles Perine, Lord Remorin, Martin Rösler, and Rainer Vosseler. (n.d.). Caught in the Act: Running a Realistic Factory Honeypot to Capture Real Threats. Retrieved April 12, 2021. (https://documents.trendmicro.com/assets/white_papers/wp-caught-in-the-act-running-a-realistic-factory-honeypot-to-capture-real-threats.pdf)
10. a b Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, Christopher Glyer. (2017, December 14). Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. Retrieved January 12, 2018. (https://www.firee

19. ^ Lee Mathews. (2016, April 27). German nuclear plant found riddled with Conficker, other viruses. Retrieved October 14, 2019. (https://www.geek.com/apps/german-nuclear-plant-found-riddled-with-conficker-other-viruses-1653415/)
20. ^ Sean Gallagher. (2016, April 27). German nuclear plant's fuel rod system swarming with old malware. Retrieved October 14, 2019. (https://arstechnica.com/information-technology/2016/04/german-nuclear-plants-fuel-rod-system-swarming-with-old-malware/)
21. ^ Dark Reading Staff. (2016, April 28). German Nuclear Power Plant Infected With Malware. Retrieved October 14, 2019. (https://www.darkreading.com/endpoint/german-nuclear-power-plant-infected-with-malware/d/d-id/1325298)
22. ^ BBC. (2016, April 28). German nuclear plant hit by computer viruses. Retrieved October 14, 2019. (https://www.bbc.com/news/technology-36158606)
23. ^ ESET. (2016, April 28). Malware found at a German nuclear power plant. Retrieved October 14, 2019. (https://www.welivesecurity.com/2016/04/28/malware-found-german-nuclear-power-plant/)
24. a b c Marshall Abrams. (2008, July 23). Malicious Control System Cyber Security Attack Case Study– Maroochy Water Services, Australia. Retrieved March 27, 2018. (https://www.mitre.org/sites/default/files/pdf/08_1145.pdf)
25. ^ Bastille. (2017, April 17). Dallas Siren Attack. Retrieved November 6, 2020. (https://www.bastille.net/blogs/2017/4/17/dallas-siren-attack)
26. ^ Zack Whittaker. (2017, April 12). Dallas' emergency sirens were hacked with a rogue radio signal. Retrieved November 6, 2020. (https://www.zdnet.com/article/experts-think-they-know-how-dallas-emergency-sirens-were-hacked/)
27. ^ Enterprise ATT&CK. (2019, October 25). Spearphishing Attachment. Retrieved October 25, 2019. (https://attack.mitre.org/techniques/T1193/)
28. a b Control Global. (2019, May 29). Yokogawa announcement warns of counterfeit transmitters. Retrieved April 9, 2021. (https://www.controlglobal.com/industrynews/2019/yokogawa-announcement-warns-of-counterfeit-transmitters/)
29. ^ F-Secure Labs. (2014, June 23). Havex Hunts For ICS/SCADA Systems. Retrieved October 21, 2019. (https://www.f-secure.com/weblog/archives/00002718.html)

ye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html)

11. ^ Dragos. (2017, December 13). TRISIS Malware Analysis of Safety System Targeted Malware. Retrieved January 12, 2018. (https://dragos.com/blog/trisis/TRISIS-01.pdf)
12. ^ Pinellas County Sheriff’s Office. (2021, February 8). Treatment Plant Intrusion Press Conference. Retrieved October 8, 2021. (https://www.youtube.com/watch?v=MkXDSOgLQ6M)
13. a b Department of Justice (DOJ), DHS Cybersecurity & Infrastructure Security Agency (CISA). (2021, July 20). Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013. Retrieved October 8, 2021. (https://us-cert.cisa.gov/sites/default/files/publications/AA21-201A_Chinese_Gas_Pipeline_Intrusion_Campaign_2011_to_2013%20(1).pdf)
14. ^ Kernkraftwerk Gundremmingen. (2016, April 25). Detektion von Büro-Schadsoftware an mehreren Rechnern. Retrieved October 14, 2019. (https://www.kkw-gundremmingen.de/presse.php?id=571)
15. ^ Trend Micro. (2016, April 27). Malware Discovered in German Nuclear Power Plant. Retrieved October 14, 2019. (https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/malware-discovered-in-german-nuclear-power-plant)
16. ^ Christoph Steitz, Eric Auchard. (2016, April 26). German nuclear plant infected with computer viruses, operator says. Retrieved October 14, 2019. (https://www.reuters.com/article/us-nuclearpower-cyber-germany/german-nuclear-plant-infected-with-computer-viruses-operator-says-idUSKCN0XN2OS)
17. ^ Catalin Cimpanu. (2016, April 26). Malware Shuts Down German Nuclear Power Plant on Chernobyl's 30th Anniversary. Retrieved October 14, 2019. (https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml)
18. ^ Peter Dockrill. (2016, April 28). Multiple Computer Viruses Have Been Discovered in This German Nuclear Plant. Retrieved October 14, 2019. (https://www.sciencealert.com/multiple-computer-viruses-have-been-discovered-in-this-german-nuclear-plant)

30. ^ North American Electric Reliability Corporation. (2021, June 28). Glossary of Terms Used in NERC Reliability Standards. Retrieved October 11, 2021. (https://www.nerc.com/files/glossary_of_terms.pdf)
31. ^ Alexander Bolshev, Gleb Cherbov. (2014, July 08). ICSCorsair: How I will PWN your ERP through 4-20 mA current loop. Retrieved January 5, 2020. (https://www.blackhat.com/docs/us-14/materials/us-14-Bolshev-ICSCorsair-How-I-Will-PWN-Your-ERP-Through-4-20mA-Current-Loop-WP.pdf)
32. ^ Alexander Bolshev. (2014, March 11). S4x14: HART As An Attack Vector. Retrieved January 5, 2020. (https://www.slideshare.net/dgpeters/17-bolshev-1-13)
33. a b John Bill. (2017, May 12). Hacked Cyber Security Railways. Retrieved October 17, 2019. (https://www.londonreconnections.com/2017/hacked-cyber-security-railways/)
34. ^ Shelley Smith. (2008, February 12). Teen Hacker in Poland Plays Trains and Derails City Tram System. Retrieved October 17, 2019. (https://inhomelandsecurity.com/teen_hacker_in_poland_plays_tr/)
35. ^ Bruce Schneier. (2008, January 17). Hacking Polish Trams. Retrieved October 17, 2019. (https://www.schneier.com/blog/archives/2008/01/hacking_the_pol.html)

Retrieved from "https://collaborate.mitre.org/attackics/index.php?title=Initial_Access&oldid=7068"

This page was last edited on 4 December 2019, at 12:56.

This page has been accessed 13,614 times.