



ICSJWG Quarterly Newsletter

ICSJWG 2010 Fall Conference

The ICSJWG 2010 Fall Conference is quickly approaching! If you have not yet registered for the conference, you can do so at http://www.us-cert.gov/control_systems/icsjwg/conference.html. Registration can be made on-site and up to the date of the conference. The conference will be held in Seattle, WA at the Renaissance Seattle Marriott Hotel from October 25-28, 2010. The hotel will honor the FY2011 per diem rate of \$139/night for federal employees with personnel badge or ID card.

- **October 25, 2010:** This day is set aside for subgroup working meetings.
- **October 26, 2010:** Official conference kickoff with plenary sessions, subgroup presentations, and speakers from industry and government. This year we will also have an informal Tools and Remediation Hands-on Workshop on Stuxnet following the general presentations.
- **October 27, 2010:** The second day of the conference includes three tracks of presentations from industry and government.
- **October 28, 2010:** Optional *Introduction to Industrial Control Systems Cyber Security Training*. You can register for the training separate from the conference. There is no fee for either the conference or the training, but meals and accommodations are the responsibility of the participant.

The draft agenda for the Fall Conference in Seattle is located on the HSIN Portal at:

<https://cs.hsin.gov/C10/C1/ICSJWG/Lists/Announcements/DispForm.aspx?ID=8&Source=https%3A%2F%2Fcs%2Ehsin%2Egov%2FC10%2FC1%2FICSJWG%2Fdefault%2Easpx>

For those who are speaking at the conference, please send your presentation to icsjwg@dhs.gov by **October 8, 2010**. We appreciate those who have volunteered to share their time, knowledge, experiences to contribute to this shared mission.

Each subgroup needs to prepare a presentation for the subgroup presentation. The deadline for subgroup presentations is **October 8, 2010**.

About the ICSJWG

The ICSJWG is a collaborative and coordinating body operating under the Critical Infrastructure Partnership Advisory Council (CIPAC) requirements. The ICSJWG provides a vehicle for communicating and partnering across all critical infrastructure and key resources (CIKR) sectors between federal agencies and departments as well as private asset owner/operators of industrial control systems. The goal of the ICSJWG is to continue and enhance the facilitation and collaboration of the industrial control systems stakeholder community in securing CIKR by accelerating the design, development, and deployment of secure industrial control systems.

*For more information, visit
http://www.us-cert.gov/control_systems/icsjwg/*

ICSJWG Subgroup Status

Below is an update on the progress of these subgroups. If you would like to become a member in any of the subgroups, send an email with your contact information to: icsjwg@dhs.gov.

➤ **Information Sharing Subgroup**

GCC Co-Chair: George Bamford
SCC Co-Chair: VACANT

The group sponsored the ICSJWG HSIN site, which is now up and running. The group has arranged for the HSIN administrator to give a demonstration at the Fall Conference on how to use the portal. If you have any feedback for methods for sharing information and improving communications using HSIN please send your ideas to icsjwg@dhs.gov.

Nathan Faith resigned as the SCC co-chair. If you would like to nominate yourself or someone else to this position, please email icsjwg@dhs.gov with your recommendation.

➤ **International Subgroup**

GCC Co-Chair: Rick Lichtenfels
SCC Co-Chair: Graham Speake

DHS is placing the monthly International Subgroup meetings on hold. Due to the logistics of coordinating meetings across the 24 different time zones, it was difficult to find a regular meeting time. The International Subgroup workspace will remain on HSIN for members who want to collaborate on international issues.

➤ **Research and Development Subgroup**

GCC Co-Chair: Dr. Douglas Maughan (Douglas.Maughan@dhs.gov)
SCC Co-Chair: David L Norton (DNORTOI@entergy.com)

The Research & Development subgroup continues to focus on objective #1 in their charter, which is to identify existing and planned R&D needs and priorities as they relate to ICS. The group agreed that they need input from owners and operators as well as further discussions with vendors. Completing this objective will help to drive the R&D subgroup closer to its larger goals. This group is looking to increase its membership.

➤ **Roadmap to Secure Industrial Control Systems**

GCC Co-Chair: Perry Pederson (perry.pederson@nrc.gov)
SCC Co-Chair: Tim Roxey (Tim.Roxey@nrc.net)

The Roadmap subgroup has been actively meeting on the second Thursday of every month to adjudicate the many comments that have been received on the *Cross-Sector Roadmap to Secure Control Systems* document. The subgroup has made good progress on the document, and many of the comments were well-received. The final document is scheduled to be published in 2011.

The group also continues to meet on the fourth Thursday of every month to discuss general items. The Roadmap sub-group has decided to hold their working meeting at the conference

from 1-4 pm PST on Monday, October 25, 2010.

➤ **Vendor Subgroup**

GCC Co-Chair: Rick Lichtenfels (cssp@dhs.gov)

SCC Co-Chair: Eric Cosman (ECCosman@dow.com).

The Vendor subgroup continues to meet at 2 pm on the fourth Thursday of each month. Over the last couple of meetings, the group engaged in discussions ranging from vulnerability disclosure/handling process to cross organization trusted identity. Another topic of discussion was the relationship amongst subgroups. Whereas the other subgroups are task-based groups, the Vendor subgroup identified themselves as more of an expertise-based advisory group to the other subgroups. For example, as solution providers, the Vendor subgroup could help the R&D group focus on particular research efforts or provide input to the Roadmap Subgroup's *Cross-Sector Roadmap* document. These topics will be discussed further at the face-to-face meeting at the conference. The group is looking to meet on the morning of October 25, 2010, although a specific meeting time has not yet been determined.

➤ **Workforce Development Subgroup**

GCC Co-Chairs: Ben Wible (wibleb@ndu.edu) and Dr. John Saunders (saunders@ndu.edu),

SCC Co-Chair: Marcus Sachs (marcus.sachs@verizon.com).

The co-chairs have devised nine task groups revolving around the requirements and working objectives of the subgroup.

1. Begin coordination and integration with external subgroups.
 - Vendor subgroup (skills gaps)
 - Research and Development subgroup (skill gaps)
2. Reach out to the Institute for Infrastructure Protection (I3P).
3. Coordinate with the International Subgroup.
4. Research and provide information to the working group on the Federal Government's effort (OPM & DHS) to create classifications, job descriptions, etc. for the generic security workforce.
5. Research and provide information to the working group regarding a certification in SCADA Security by Exida. It falls in line with their CFSE & CFSP certification for individuals.
6. Create a diagram of some sort that shows the path and career fields from high school graduate working as an apprentice or intern all the way to Plant Control Officer (or whatever the most senior ICS/PCS security person would be called in the Plant.)
From there we will start dividing into technicians, engineers, managers, support, executives, etc.
7. Plan for moving forward on our second task: gap analysis. This task should cover both certification and academic.

8. Plan and design for three sets of curriculum
 1. Executives
 2. Control System Engineers & Technicians
 3. IT/Computer Science Personnel

*Numbers 2 & 3 could be combined to create a 40xx Training standard.
9. Write a white paper capturing research accomplished by the working group. Provide overview of workforce training and certifications. This should be a “living document that continues to be upgraded as we move forward.

The subgroup is still looking for additional volunteers to help work on these tasks. If you would like to assist with any of the Workforce Development tasks, email wibleb@ndu.edu.

The group has also been in contact with the Institute for Information Infrastructure Protection (I3P). The I3P includes members of over 25 colleges and universities who expressed interest in working with the Workforce Development subgroup; they have been working on a workforce development project for the last four to five years, mostly in the oil and gas arenas. Currently, the challenge is for them to get funded to be able to work with the Workforce Development subgroup.

The group is looking to meet October 25, 2010 from 1-4pm.

Homeland Security Information Network (HSIN)

HSIN is now fully developed and in use. ICSJWG subgroup members may send an email to icsjwg@dhs.gov to request an account.

- **If you do not currently have a HSIN account**, please provide your name, company, contact information, critical infrastructure sector, and ICSJWG subgroup affiliations.
- **If you already have an HSIN account**, please provide your name, HSIN user name, ICSJWG subgroup affiliation, and critical infrastructure sector.

Individual subgroup folders have been set up to facilitate subgroup collaboration. Inside the respective folders, users will find meeting minutes, working documents, subgroup roster, and charter, amongst other documents. HSIN also features a calendar listing monthly subgroup meetings, ICSJWG events and deadlines. Other capabilities of this portal include a discussion board and webinar capability.

Based on feedback submitted by ICSJWG HSIN users, DHS is already working with HSIN administrators to make some improvements to the portal. Some of the changes include making the subgroup “workspaces” more functional by providing each subgroup workspace with its own calendar, document library, link to webinars, contact list, and discussion board. DHS expects to have these changes in place by the conference.

Keep abreast of what’s happening by taking advantage of HSIN’s Alerts feature. By activating this setting, you can obtain status on what content has been added or modified. You can set up alerts to notify you of changes immediately as they happen, or get daily or weekly summaries.

Submit an Article to the ICSJWG Newsletter

As a reminder, ICSJWG is accepting short articles of general interest pertaining to control systems security for our quarterly newsletter. If you want to submit an article for our December newsletter, please email icsjwg@dhs.gov, and we will take your article into consideration for publishing. The deadline for submissions for the December newsletter is **November 19, 2010**.

Past ICSJWG newsletters are located on the CSSP website at http://www.us-cert.gov/control_systems/icsjwg/index.html and on HSIN at <https://cs.hsin.gov/C10/C1/ICSJWG/default.aspx?RootFolder=%2fC10%2fC1%2fICSJWG%2fDocument%20Library%2fICSJWG%20Newsletters&View=%7b7F0225B9%2d1943%2d4074%2dB349%2d32C32A4EB8E7%7d>.

Training Events Scheduled for 2010

CSSP is currently offering advanced and introductory cyber security training. There is no cost to attend the training; however, travel expenses and accommodations are the responsibility of each participant. Additional offerings are being planned for next year and will be announced once dates are finalized. More information, including registration and future offerings, is available at: http://www.us-cert.gov/control_systems/.

Introductory Training

This course is directed to those with IT Security responsibilities or background but have no previous experience in critical infrastructure control systems and their relationship to modern IT networks.

Four training modules will guide attendees from basic definitions, components, and protocols to the major applications and architectures within critical infrastructure (CI) and key resources (KR). Control system network architectures, cyber threats and vulnerabilities, and mitigations will be presented. Current and emerging government and industry activities that are addressing the issue of risk reduction will be discussed.

The following introductory training events have been scheduled for the remainder of 2010:

- **October 28, 2010 – Seattle Washington:** Everyone
- **November 18, 2010 – Arlington VA:** Federal Partners

Advanced Training

This event will provide intensive hands-on training on protecting and securing control systems from cyber attacks, including a very realistic Red Team / Blue Team exercise that will be conducted within an actual control systems environment. It will also provide an opportunity to network and collaborate with other colleagues involved in operating and protecting control systems networks.

The following advance training events have been scheduled for the remainder of 2010:

- **November 15-19, 2010:** US Asset Owners and Vendors
- **December 6-10, 2010:** US Asset Owners and Vendors

The training is held at the Control Systems Analysis Center located in Idaho Falls, Idaho, and

provides an intensive, hands-on environment. Students gain experience protecting and securing industrial control systems from cyber attacks, including s Red Team /Blue Team exercise that are conducted within an actual control systems environment.

Industrial Control Systems Articles

The following articles were submitted by members of the ICSJWG for publication. Thank you for contributing.

DHS Hosts ICS Roadmap Implementation Workshop

Chemical Sector Specific Agency

On July 9, 2010, the U. S. Department of Homeland Security (DHS) hosted a one-day facilitated cross-sector workshop for control systems security experts. With an environment that is rapidly changing in terms of threats, technology advancements, and policies, cybersecurity experts are seeking to better leverage resources to accelerate progress in achieving a common vision of control systems security. Participants engaged in discussions aimed at identifying and leveraging opportunities to coordinate and implement activities to secure control systems across multiple sectors.

Participants acknowledged the importance of technology development in securing control systems. However, as potential first steps, attendees identified the following outreach and awareness opportunities:

- Building a business case for investment in cybersecurity;
- Fostering a culture change with respect to cybersecurity;
- Encouraging a cross-sector awareness campaign; and
- Creating a forum to enhance collaboration and develop methods of tracking progress.

Participants agreed that continuing engagement in cross-sector forums is necessary to fully optimize the diverse, yet limited resources, found in each sector.

Remote Assistance and Remote Monitoring in the Age of Industrial Cyber Security

By Lior Frenkel, Co-Founder and CEO, Waterfall Security Solutions

Background

As Critical National Infrastructure owners, utilities are mandated to maximize the uptime, performances and integrity of the mission critical equipment such as power turbines, industrial and control networks, and applications. This need is, in many cases, a requirement of regulatory authorities such as NERC, NRC and others. They need to continuously monitor the equipment and to be able to react very quickly in case of equipment malfunction. There are different technical teams which are involved in the maintenance processes. In some cases these procedures are being done by the utility's in-house technical teams and in others, by equipment manufacturers, vendors or by 3rd

party technical support teams.

Quite often, these technical support teams are not located in the same site as the equipment. They might even be located thousands of miles away. To overcome this, the utilities are making broad use of remote assistance services as it enables them to run the operation processes effectively and to maximize machine uptime.

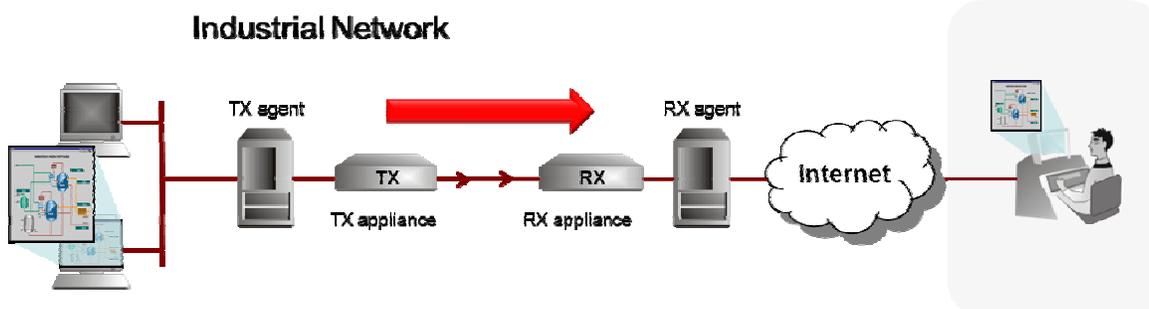
Current status

The use of remote assistance requires direct access of the technical support teams to the utility's mission critical infrastructure located in the industrial network. This access, done over public networks, exposes the industrial network to threats of cyber-attacks, virus infiltration, malware penetration and human errors. Such threats may result in power outages, loss of revenue and other sorts of damages. Moreover, with the growing concern of the North-American authorities and regulators, regarding the vulnerability of the Critical Infrastructure Industrial networks, utilities are required to meet the compliance requirements of NERC-CIP, NRC, CFATS and other regulations.

The common ways to protect the remote monitoring process is using IT security products and technologies, which are all software based. Software based security does not provide adequate protection as it carry inherent vulnerabilities, such as: software bugs or miss-configuration, exploits and vulnerabilities. Modern cyber security and overall reliability requirements have driven both the utilities and the relevant regulators to an understanding that IT security does not provide adequate security resilience.

New trends in security

Today a new breed of products, Unidirectional Security Gateway (USG), offers the industrial networks absolute security, yet it maintains full data visibility needed for remote assistance.



The unidirectional security gateway is composed of two appliances - (TX appliance and RX appliance), and two software agents which are installed on dedicated local servers. The connection between the TX appliance and RX appliance is done using a unidirectional fiber optic link.

The appliances are hardware based communication systems that provide unidirectional, high speed data connectivity. To guarantee the unidirectional data flow, the TX appliance hardware supports only the transmitting LED where the RX appliance hardware supports only the receiving photo-transistor module. Consequently, transmission of data from the less secured network towards the industrial network is physically impossible. It preserves industrial network segregation from external networks, and protects the utilities' critical assets from any threat of cyber-attacks, incoming viruses and malware or human errors. Moreover, it assists the utilities to address the NERC-CIP, NRC, CFATS and other regulation, compliance framework requirements.

One critical issue is that the Unidirectional Security Gateway will retain the reliability, uptime, and performance of the remote assistance application. The gateway replicates, in real-time, servers and workstations' screens located in industrial networks to external networks. The remote technical support can view, in real time, system status, application HMI's and other displayable information. To support the diverse performances and usability needs, of the utility's industrial network and the

public data networks, the gateway provides a wide range of functionality and configurations needed for effective monitoring and operational processes support.

Summary

Utilities make use of remote assistance in order to maximize the reliability and uptime of their mission critical infrastructure. This, however, exposes the networks to threats of cyber- attacks, intrusions through external networks, viruses or human error. Recent cyber security “issues” prove this risk is real and actual. Having to provide adequate cyber security level while keeping reliability and maintainability intact, faced them with the Catch-22 situation.

The hardware based, unidirectional security gateway, helps the utilities to solve the dilemma as it provides the industrial network absolute cyber security while it maintains real time remote assistance ability, and helps to meet the regulations demands.

APT (Advanced Persistent Threats) and How They Impact SCADA and ICS Systems

Jonathan Pollet, CISSP, CAP, PCIP

Joe Cummins, PCIP

What is APT?

The Advanced Persistent Threat (APT) is a new type of attack on Corporate IT systems that leverages the latest advanced cyber security and espionage techniques to gain a foothold on the system. It is persistent because the attacker leaves behind back doors and root kits that allow the attacker to move effortlessly in and out of the system. The threat is real, and unfortunately many are not aware that their systems have been compromised until they realize that they are not in control of their own systems anymore.

One of the fundamental things that set apart the APT threat from others is that individuals are not carrying out these attacks working alone. They appear to be the result of a well-funded, well-organized group of attackers. It starts small, but then the victim realizes that as they change core administrator accounts and passwords, someone or something is changing them back. New administrator accounts are created daily. Any attempt to root out the unknown presence on the system is quickly foiled and the threat advances to the point where the user and administrators of the system are no longer in control of the system.

This is happening right now to thousands of companies around the world, and several large Fortune 50 corporations are now completely no longer in control of their systems. They have also determined that the core images that they use to build new workstation and server builds are also compromised with the APT threat so that as new systems come on-line, they are already available for use by the attacker.

To make things worse, these APT attacks have extended down into the SCADA and real-time environments. We have been involved in incidents whereby SCADA, DCS, and process control systems have been infected with APT malware and C&C code that allow the attackers to remotely control the system.

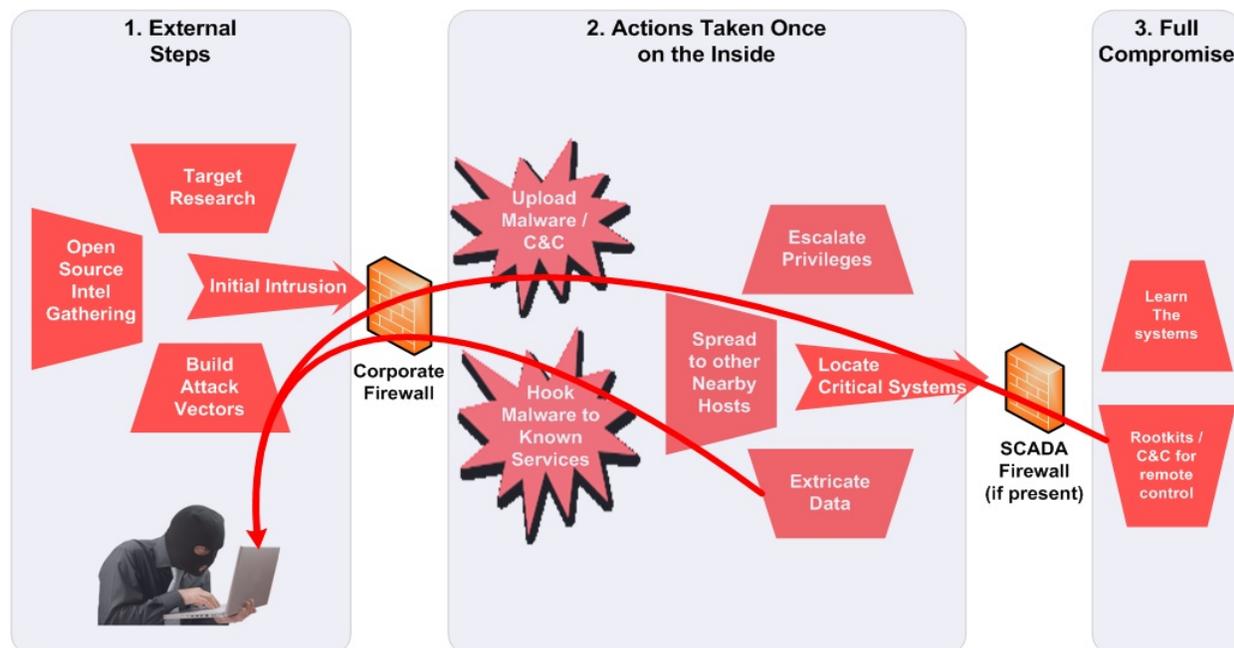
APT Attack Methodology

Advanced Persistent Threats make use of various public source intelligence gathering techniques to research viable targets, and then build specific attack vectors tailored to the target. In many cases, the initial intrusion is made through a spear-phishing campaign. It only takes one initial intrusion to allow the attacker to upload malware to the target network.

The unique thing about APT attacks is that the malware or payload is almost always hooked to known system services in an attempt to hide its presence. This not only allows the attacker to evade antivirus detection techniques, but also makes it difficult to determine if a system has been compromised. The malware usually contains command and control capabilities as well as the ability for the attacker to gain remote access to the compromised system again in the future.

Once their presence is sustained on the network, then APT attacks will then escalate their privileges on the system and expand the attack footprint. This is often achieved by deploying C&C (command and control) nodes that take on roles as “commanders” and “drones.” The local commanders on the network can be used to provide localized command and control capabilities deep within the targeted network. The “commanders” have the ability to create “drones” and pass along instructions on how and when to ping back to external servers. Instead of a barrage of constant attacks and malware updates, APT attacks use a “low-and-slow” approach. In some cases, drones have been known to stay dormant for over 12 months while waiting to be awakened.

The goal of this attack is to maintain a presence on the targeted network without detection, while leveraging the local presence to extract useful information or locate mission critical systems such as SCADA, DCS, or highly critical applications. Once these sensitive and critical systems are located, the presence on the network is maintained so that in some future time, those critical systems can be compromised. The typical APT attack methodology is depicted below:



How to Detect an APT Attack

If you suspect that your systems may have been compromised by an APT attack, your job has just become much more difficult than you can imagine. System logs may not even show it. APT attacks

often masquerade as legitimate network traffic, and the malicious payload often hooks itself to known system processes.

The best way to verify if there has been a compromise is to place a sniffer on the outbound side of the Internet firewall, and also step up the outgoing traffic monitoring. Start to model what the “normal” destinations are for corporate traffic, and use a process of elimination to get to the point where suspicious outbound traffic can be further evaluated.

Packet captures, network device logs, and internal host event log activity can be good tools to determine what is going on. If your company or organization is not logging network activity or keeping system logs on their servers and workstations, you may never be able to determine if your company is a victim of an APT attack.

Another sign that your organization may be already compromised is if unauthorized changes are being made to any system accounts. If new domain controller accounts are added to the system, if user accounts are randomly locked, then unlocked, or if the administrator account starts to be used when the administrators are clearly not on the network, then the APT attacker has already established a bi-directional link with the network, and can remotely log into the system, and control the systems on the corporate IT network.

Making sure that all critical host systems have system logging enabled and configured properly is important. The logs should also be exported on a routine basis to a centralized log server. Many times the attacker will be smart enough to clean up their tracks. The logs on the local servers and workstations may look clean, and locked accounts can also be unlocked so that there is little trace that the attacker was on the system. If the activity on the servers and workstations are logged to a centralized log and alert management system, then all host activities are logged in a secondary location.

Another good indicator that your system has been compromised by an APT attack is by analyzing one of the servers or workstations that you believe has been involved in the attack. Typically the logs will point out specific systems by IP address on the inside of your network that was exporting data or used to escalate system privileges. Often, the malware and command and control (C&C) rootkits used by APT are not discovered by rootkit detectors, so in order to be absolutely sure that the system has been compromised, we found that it is best to analyze the file size and number of instances of the following filenames on Windows systems:

- svchost.exe (most common)
- iexplore.exe
- iprinp.dll
- winzf32.dll

By using a combination of several network and host investigative tools, you can determine how many instances of these files are running in memory, the size of those files, and what specific process identifiers (pids) are associated with them. Typically APT attacks will hook their malware and C&C software to those processes listed above.

How to Determine How Far the APT Attack has Spread

Once the above steps are used to determine the initial attack vector, and what systems on the internal network are infected, the next step is to discover how far the APT attack has spread throughout the network.

In almost all APT incidents that we have been involved with, there has been an initial attack vector, followed by implementation of malware and C&C code that allows the attacker to spread the infection onto other nearby systems. By using the concept of “Commanders” and “Drones” the initial dropper can then be activated to perform tasks for the attacker that include creating and deploying drones that infect other nearby systems and then report back to the “Commander” or back to the attacker through an outbound connection to an external site.

Once a system has the malware or C&C code, and has been designated as “Commander” or as a “Drone” then the attacker uses these internal servers or workstations for the following purposes:

1. Spread the surface of the attack to other systems on the network
2. Locate interesting data such as corporate emails, sensitive documents, batch recipes, and any intellectual property that might be valuable
3. Locate other critical systems such as building automation controls, security alarm systems, badge access systems, SCADA, DCS, and process control systems, and anything else that can be useful to have remote command and control over
4. Begin extracting internal sensitive data, emails, and real-time SCADA tag values to external servers

Before pulling the plug on the APT attack in an attempt to root out the attacker, it is important to understand the full extent of the attack so that as the containment process begins, future work by the attacker to continue its persistence on the network can be mitigated.

We have found that **leveraging both Network and Host-based tools** are the key to identifying how far the infection has spread in the system. We have also created a very passive approach to detect the presence of APT without affecting the performance of the system or alerting the attacker to the discovery techniques.

The Red Tiger Security team has used this passive approach to investigate several SCADA and DCS systems to discover the presence of an APT threat agent within the control systems. In each example, the team was able to move inside the control system, collect the forensic and real-time network and host data required for analysis, and leave the control room environments all without **impacting the SCADA or DCS systems in use.**

Summary Remarks

The threat of an APT (Advanced Persistent Threat) is real and APT attacks are ongoing even to the present day on several large Fortune 50 corporations. APT attacks are difficult to detect, difficult to prevent, and requires a sophisticated and planned remediation scheme that not only addresses repairing the external perimeter access into the network, but also hardening internal systems to prevent additional APT outbreaks.

What we have learned from analyzing APT threats include the following:

- The attacker typically targets mostly large Fortune 50 or Fortune 500 companies, often based on current events or specific intelligence data that is desired about the victim company
- Senior executives are often targeted with spear phishing attacks as the initial intrusion vector

- The APT attackers often leverage valid accounts, escalate privileges, and then move laterally inside the internal network with the motivation to:
 1. Spread the surface of the attack to other systems on the network
 2. Locate interesting data such as corporate emails, sensitive documents, batch recipes, and any intellectual property that might be valuable
 3. Locate other critical systems such as building automation controls, security alarm systems, badge access systems, SCADA, DCS, and process control systems, and anything else that can be useful to have remote command and control over
 4. Begin extracting internal sensitive data, emails, and real-time SCADA tag values to external servers

- Leveraging both Network and Host tools can be the most effective method to determine what systems have been compromised

- Remediation of APT attacks must be a coordinated, well-planned, and well-executed process; otherwise the threat will use various covert methods to retain their persistence on the network.

- When SCADA, DCS, or process control systems are at risk, those systems must be allowed to continue to operate while the APT investigation is ongoing, so utilizing a passive approach that does not impact the control systems is paramount.

Participation is Key!

Your participation and input is **critical** to the success of these subgroups and to the overall mission of ICSJWG to coordinate cyber security efforts to secure ICS across the nation's critical infrastructure. Please email the co-chairs or icsjwg@dhs.gov to get involved with one or more of the subgroups.

Contact Information

If you would like to contact the ICSJWG to ask a question or inquire about participation, please send an e-mail to icsjwg@dhs.gov.

The CSSP and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) encourage you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems. Online reporting forms are available at <https://forms.us-cert.gov/report/>.

Other important contact information:

Web Site Address: http://www.us-cert.gov/control_systems/

ICS-CERT Email: ics-cert@dhs.gov

Phone: 1-877-776-7585

CSSP Email: cssp@dhs.gov