OVERVIEW

Cb Protection provides industrial control system operators with real-time visibility and proactive, customizable signature-less protection from advanced persistent threats. Leveraging three distinct forms of application control, Cb Protection continuously protects on-network, off-network, and air-gapped critical infrastructure deployments from today's known and tomorrow's unknown threats.

HIGHLIGHTS

- Prevent advanced persistent threat and zero-day attacks.
- Stop malicious, illegal or unauthorized software from running.
- Gain real-time visibility into all files, applications and executables in your environment.
- Ensure regulatory compliance with streamlined auditing and activity monitoring
- Lock down disconnected devices to prohibit unauthorized change.
- Eliminate risk associated with portable storage devices.
- Integrate with leading network, SIEM and analytic security platforms.
- Trusted by some of the world's largest utilities and industrial organizations to protect ICS/SCADA systems against advanced attacks.

Critical Infrastructure Control Systems

Preventing Attacks on Critical Infrastructure Control Systems

Critical industrial and infrastructure control systems face increasingly sophisticated cyber attacks. Designed to leverage cyber assets to inflict physical damage upon infrastructure systems or the products/goods they support, advanced cyber attacks are a real and growing threat to public utilities, transportation systems, water treatment plants, communication networks, and large manufacturing facilities. As cyber attacks have transformed from being an IT problem to an organizational and national security risk, the consequences of having insecure industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems can be devastating, impacting far more than an organization's bottom line.

"Industrial Control Systems are increasingly under attack by a variety of malicious sources. These attacks range from hackers looking for attention and notoriety to sophisticated nation-states intent on damaging equipment and facilities, disgruntled employees, competitors, and even personnel who inadvertently bring malware into the workplace by inserting an infected flash drive into a computer."

– ***Charles Edwards,*** Deputy Inspector General, US Department of Homeland Security.

Industrial Control Systems are Under Attack

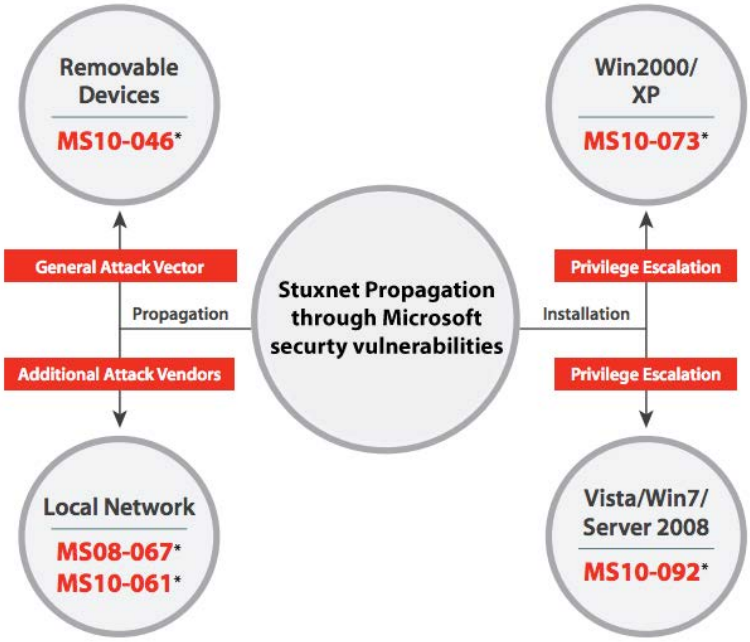
Most ICS or SCADA implementations were designed when external, malicious cyber attacks were not considered a possibility, let alone a viable threat. While most operators of these systems have come to recognize the risk posed by advanced attacks, far fewer have implemented pro-active security policies, at the endpoint, capable of preventing the most dangerous attacks. This is proving increasingly dangerous, as advanced attackers become more adept at finding vulnerabilities in network defenses and by-passing signature based solutions, such as anti-virus.

With the ability to by-pass security barriers and spread across devices with invisibility, the weapons and tactics of cyber attacks used by well-funded nation states to penetrate and compromise critical systems are now intricate and multi-layered. These attacks are capable of penetrating the most complex architectures, even devices completely disconnected from the corporate network, and are consistently building strength, the most well-known of these types of attacks being the Stuxnet virus.

Carbon Black.

Looking Deeper into Recent Control System Attacks

In December 2015 hackers caused an outage at a Ukranian power plant that impacted 700,000 customers by targeting the plant's SCADA system. It was also recently disclosed that at least two US airports had fallen victim to an advanced malware attack through a phishing attack directed at aviation personnel. Around the same time, the Department of Homeland Security announced it was investigating a string of Havex Trojan attacks that had used phishing and software vendor updates to target oil and gas companies in the United States and Europe. Earlier in 2014, the US Department of Justice indicted five Chinese military officials on charges of hacking into US critical infrastructure systems. While these are just a few examples of how attackers are adopting increasingly complex techniques to infiltrate and attack critical systems, they showcase why it is increasingly important that critical infrastructure operators both deploy pro-active and customizable prevention capabilities and build out rapid threat detection and incident response capabilities that are able to stop and kill attacks in-motion, within seconds of detection.

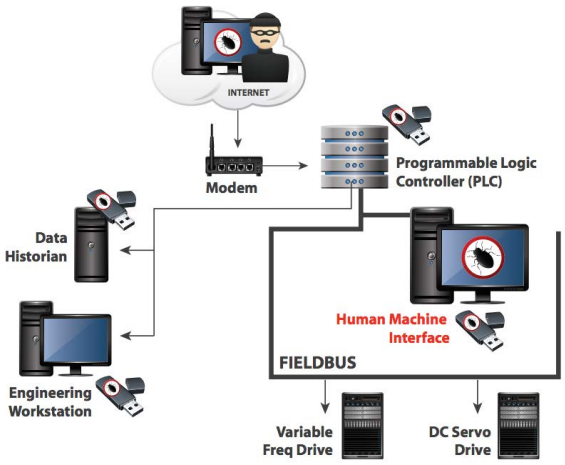


Perhaps the best known attacks on critical infrastructure were the 2010 Stuxnet worm, used to attack programmable logic controllers (PLCs) in Iranian nuclear development facilities, and the 2012 Flame virus.

Typically injected into an environment through removable media and designed to propagate–without being detected–in "sneaker-net" environments, Stuxnet was the first virus designed to inflict sabotage on industrial processes by exploiting a specific type of industrial control system software. This allows it to target software commonly used in manufacturing, utilities, and even nuclear powered aircraft carriers. With the source code now in the public domain, it is widely acknowledged that the Stuxnet virus could be reconfigured or adapted to attack critical infrastructure targets in the US, Europe, and Japan.

Antivirus is no Protection against Advanced Threats

As recent attacks and numerous research reports have shown, antivirus technologies are ineffective at stopping advanced attacks like Stuxnet and Flame. This is because antivirus software is retroactive by design and depends upon a "blacklist" of known malware. In contrast, today's advanced attacks are well planned and often use customized zero-day malware that targets specific operators or control systems and is not recognized by antivirus solutions.



According to Lastline Labs, today's antivirus solutions are only capable of detecting 51% of new malware. Clearly, when it comes to critical infrastructure a 49% failure rate is unacceptable and antivirus does nothing to thwart the loading of legitimate, but unauthorized, software that could pose a risk to the environment. In addition, antivirus solutions have often proven difficult to effectively deploy on distributed control systems (DCSs), remote PLCs, and the human machine interfaces (HMIs) that manage critical systems. Because antivirus deployments on these systems require constant testing and updating to maintain, it can serve as a significant burden on the security operations teams tasked with their defense.

KEY BENEFITS

ADVANCED THREAT PREVENTION

- Stops today's and tomorrow's advanced threats.
- Prevents zero-day attacks.
- Provides real-time visibility

LOWER COST OF SECURITY

- Centralized visibility and control of ICS/ SCADA systems.
- Proactive security greatly reduces number of IR activities.

ENSURED COMPLIANCE

- Enact event rules to automate policy controls.
- Lock down devices to ensure trusted state
- View real-time software inventory across environment.
- Control software access and updates.
- Log and report all software changes.
- Quickly assess policy violations.

"The status quo is no longer acceptable- not when there's so much at stake"

- President Barack Obama

Increasing Regulatory Requirements

In addition to the growing risk and occurrence of advanced malware attacks, new government frameworks and regulations are adding pressure to operators of critical infrastructure control systems to deploy advanced threat prevention and detection solutions. New and updated National Electric Reliability Corporation (NERC) requirements and a new cyber security framework from the National Institute of Standards and Technology (NIST) are forcing operators to not only think about protecting key systems, but building out the ability to provide real-time, visibility across their systems to aid in the rapid detection of and response to advanced attacks.

Securing Infrastructure Control Systems

One of the most common security strategies recommended by NIST, SANS, ENISA and others for protecting critical systems is the adoption of application whitelisting alongside multi-factor authentication and network firewalls.

When evaluating any application control or whitelisting solution, it is important to ensure that continuous availability is front and center and that the unique challenges associated with these systems have been considered in the design and implementation of the solution. These include:

- Support for legacy systems that have limited CPU resources available
- The ability to update the security solution and policies without rebooting
- Maintaining and enforcing security policy for disconnected or air-gapped devices, in-office or in the field.
- Ensuring the reliability and stability of the solution
- Meeting CIP standards, such as NERC and other industry or government standards or regulations.

Cb Protection solution is designed to meet all of these requirements and can help ensure the integrity of critical infrastructure systems by:

- Preventing unauthorized software: Lock down critical systems by ensuring that all new software is validated and checked against an authorized list or approved by IT before executing.
- Blocking unauthorized portable storage devices: Easily block USB drives, CDs, etc, ban or approve devices by serial number so that only pre-approved devices can execute.
- "Always-on" Recording and Auditing of all software changes: Ensure compliance and determine accountability with a comprehensive audit trail of all application changes.
- Blocking advanced threats such as Stuxnet and Flame: Carbon Black is the only security provider to have stopped Flame, Gauss, and the malware behind the RSA breach.
- Real time threat detection and response: Signature-less detection and response capabilities provide the information needed to quickly investigate and remediate attacks.

Carbon Black.

Carbon Black is the leading provider of a next-generation endpoint-security platform designed to enable organizations to stop the most attacks, see every threat, close security gaps, and evolve their defenses. The Cb Endpoint Security Platform helps organizations of all sizes replace legacy antivirus technology, lock down systems, and arm incident response teams with advanced tools to proactively hunt down threats. Today, Carbon Black has approximately 2,000 worldwide customers, including 25 of the Fortune 100 and more than 650 employees. Carbon Black was voted Best Endpoint Protection by security professionals in the SANS Institute's Best of 2015 Awards.

1100 Winter Street, Waltham, MA 02451 USA P 617.393.7400 F 617.393.7499 www.carbonblack.com