Use of HAVEX RAT to Compromise SCADA Systems

John P. Bryk

Webster University CSSS 5130

Contents

Abstract

The HAVEX Remote Access Trojan attacked SCADA systems worldwide from 2010 through today. Major anti-malware organizations agree the source of HAVEX is the Russian hacker group Energetic Bear, who may have Russian government backing. HAVEX has the ability to infect, reconnoiter networks, and exfiltrate information, as well as remain as a latent threat to SCADA systems by maintaining a covert command and control function. HAVEX is widely thought to be an attack against energy companies, but new information points to the real target as the pharmaceutical industry.

Keywords: HAVEX RAT, REMOTE, ACCESS, TROJAN, SCADA, COMPROMISE, EXPLOIT

Use of HAVEX RAT to Compromise SCADA Systems

SCADA

The Importance of SCADA

The technology that allows users to collect data from remote locations and to send operational instructions to those facilities is called Supervisory Control and Data Acquisition (SCADA), or, interchangeably, Industrial Control Systems (ICS). SCADA eliminates the need for an operator to physically maintain a presence at a distant location or even to visit those locations as long as they are under normal operations. SCADA includes an interface that allows the operator to observe and manipulate applications to control the remote facility or process. An important distinction between SCADA and software packages called SCADA is that an actual SCADA system contains the communication links and other necessary equipment to complete a process from command through execution (Boyer, 2009).

SCADA may be designed to control a single process, or a process as vast and complex as a national electric grid, petroleum pipeline system, or water distribution system. Using electricity as an example, superhuman speeds would be required to analyze processes, identify problem areas, and react to switching requirements and faults occurring at light speed within a national electrical grid. Only through the use of computerized and automated SCADA systems is it possible to exercise command and control over this enormous network.

Components of the SCADA system. An operator input device, which might consist of switches, buttons, or a computer keyboard, transmits inputs to a master terminal unit (MTU). Modern SCADA systems always consist of a computer-based MTU. The MTU contacts one or more remote terminal units (RTU) that may be sensors, executors, or a combination, and asks for status. Sending commands from the MTU to the RTU requires a communications network. The

commands sent within a network are generally very simple, therefore requiring low data rates. In many cases a voice grade telephone system of 1,200 to 9,600 bytes per second is sufficient to operate a SCADA system (Bailey, 2003).

Impact of attacks on SCADA systems. Modern society is completely dependent upon the systems controlled by SCADA networks. Any interruption to the flow of electricity, for example, creates a cascading impact upon other critical facets of daily life. Without electricity there is no water, no pumps to dispense fuel, subsequently limited transportation, the list goes on and on. America's, and many developed nations' critical infrastructures are based on normal operation of its SCADA systems.

The criticality of these systems make them an attractive target for degradation or destruction by various threat agents. A seemingly endless cycle of attacks against our critical infrastructure are conducted by groups of hackers backed by foreign governments. In October, 2014, NSA director Admiral Michael Rogers cited the effects of major cyber-attacks against the energy industry during a power grid security conference in San Antonio, Texas. Energy and power infrastructure, he warned, were not designed to be resilient to today's cyber-attacks (Paganini, 2014).

The impacts of normal component failure, disaster, or human operator error likewise can degrade or destroy SCADA systems to the same or, though our focus here will be upon intentional attack by malevolent actors.

In spite of their importance SCADA systems often are neglected when security is considered. SCADA systems were traditionally discrete (point-to-point, closed) networks, not connected to the web, and therefore generally safe from external penetration or exploitation. Increasing complexity and cost cutting efforts have resulted in larger and larger interconnected

and web-connected networks, creating a significant and attractive attack surface. Continued dependence on landline and/or modem connections offers attackers the option of "war dialing," or setting a computer to dial random numbers until another modem is reached. When a modem is located, an attempt to identify and penetrate the system is initiated. As landline modems have all but disappeared from internet use, SCADA legacy systems are perhaps the final vulnerable networks to this "old school" attack.

ADVANCED PERSISTENT THREATS (APT)

Characteristics and Origins of APTs

An APT is always a type of targeted attack, though not all targeted attacks are APTs. Targeted attacks use a wide variety of techniques, including drive-by downloads, SQL injection, malware, spyware, phishing, and spam (Symantec, 2011). APTs are multiphase attacks comprised of an initial penetration via a focused network or physical (thumb drive) attack, reconnaissance, commanding the attacked system to download additional malware, creating a clandestine access (backdoor), exfiltrating data and attempting to spread to other systems via the host. APTs are further characterized by their relentless, persistent intrusions typically targeting key users within organizations to gain access to trade secrets, intellectual property, state and military secrets, computer source code, and any other valuable information available (McAfee, 2011). Most often used in these attacks is malware referred to as a Trojan, a program containing a hidden set of instructions designed to open inside the target and to wreak havoc. STUXNET was the first publicly disclosed APT specifically targeting ICS (Rodillas, 2014). APTs are capable of remotely starting or stopping software and hardware systems. As more and more physical devices are controlled by embedded microprocessors, the potential for mayhem is high (Symantec, 2011). Stuxnet's purpose was to reprogram ICS so the equipment acted in a manner

programmed by the attacker, which was to destroy the targeted equipment.

The Remote Access Trojan (RAT)

The most current advanced threat to SCADA systems consists of Remote Access Trojan (RAT) attacks. A remote access Trojan (RAT) is a malware program that gives an intruder administrative control over a target computer. RATs are usually downloaded invisibly with a user-requested program -- such as a game -- or sent as an email attachment. Once the host system is compromised, the intruder may use it to distribute more RATs for a botnet (Definition: Remote Access Trojan, 2012).

HAVEX RAT

What is HAVEX?

HAVEX is a general purpose (RAT) with two identities, HAVEX RAT and SYSMain RAT. It is possible that the HAVEX RAT is itself a newer version of the SYSMain RAT, although both tools are still in use concurrently and have been operated by the attackers since at least 2010. HAVEX RAT exists in 25 known versions with build times up to October 2013 (Paganini, 2014). HAVEX not only steals sensitive information from infected machines; it includes a module that can spy on other ICS devices in the same network that the infected machine resides on, which clearly qualifies it as an industrial espionage tool (Marschalek, 2014).

(Symantec, 2011) describes traditional targeted attacks as short-term, immediate gratification efforts akin to looting. In comparison, modern APT incursions are designed to compromise a platform as a launching pad for multiple covert operations over an extended period of time.

Who is Behind HAVEX?

CrowdStrike (2014) said that a Russian group dubbed Energetic Bear, and alternatively by Kaspersky Labs and others as Crouching Yeti and DRAGONFLY (cf. Paganini P. , 2014), was using HAVEX malware to conduct intelligence collection campaigns aimed at various organizations world-wide with a primary focus on the energy sector (Kovacs, 2014). Symantec (2013) analysis of malware timestamps revealed the hackers worked a standard workday, from 0900-1800, Monday through Friday, in the UTC +4 time zone (one hour East of Moscow). *Figure 2- Forensic timestamp evidence*. Based on this information, it is likely the attackers are based in Russia. (Symantec, 2014).1 Though impossible to determine based on empirical evidence, efforts of this magnitude historically are backed by the resources of nation-states.

Attack Vectors

Phishing and spear phishing. Both of these attack vectors refer to emails with malevolent attachments or links to malware sites. By clicking on a link to open, the victim self-inoculates with the malware package. Attractive, general titles adorn the head of phishing attempts, a kind of pray-and-spray attack. If a specific individual or organization is targeted, spear phishing is often used. In this vector, the email will include a much more focused, apparently personal or official appearance. Often ploys such as “next year’s wage increases” or “a personal note from the Office of the CEO” will entice a user to click the poisoned link.

Once downloaded, the HAVEX RAT seeks out exploitations within the system, and follows the attack chain of events: reconnaissance, commanding the attacked system to download additional malware, creating a (backdoor), exfiltrating data, and attempting to spread to other systems via the host. *Figure 3- HAVEX RAT penetration*

[1] Figure 1 also indicates that they have embraced the concept of flex-time.

Strategic Web Compromises (SWC) and Watering Holes

Some organizations are security aware and resistant to phishing and spear phishing. To bypass their security, strategic web sites not a part of the target organization are compromised with malware. These sites are of a nature that the target organizations will have one or more members who visit the site during the reconnaissance and penetration phases. A number of legitimate sites were HAVEX compromised for use as SWCs (Paganini P. , 2014). SWCs are also known as "watering hole" attacks, lying in wait in an area frequented by victims. For example, an energy company would be extremely interested in new petroleum finds. A malevolent actor might attack the website carrying the story of a new oilfield with the assurance that several, if not many, victims from the target might visit this site. By simply arriving at the site or by clicking a link, i.e., "read the whole story here," the malware is downloaded and begins its attack and reconnaissance within the target system.

Vendors as Vectors. According to Kovacs (2014), Energetic Bear exploited vulnerabilities in ICS vendor websites. Upon gaining access to the sites, HAVEX was installed and the malware awaited contact by victims seeking downloads of software and patches. These vendors were based in Belgium, Switzerland, and Germany. Two of them supply remote management software for ICS and the other specializes in the development of high-precision industrial cameras. A download from an infected SCADA vendor carried the command: mbcheck.dll,RUNDllEntry, which auto-ran and created the backdoor access to the victim's machine. A clean software installation would not have include this (Hentunen, 2014).

CrowdStrike (2014) found that HAVEX variants had compromised hosts in 23 countries since 2011. While Crowdstrike identified the energy sector as the primary target, other attacks

occurred against European governments (especially Eastern Europe), defense contractors, and IT providers. Other impacted groups included European, U.S., and Asian academia, European, U.S., and Middle Eastern manufacturing and construction industries, U.S. healthcare providers, non-European precision machinery tool manufacturers, and research institutes.

According to NETRESEC's blog (Hjelmvik, 2014) the mbCHECK version for users in Europe was infected with HAVEX, but not the one for the U.S. and Canada. These facts indicated that the Dragonfly / Energetic Bear threat actor seems to primarily target ICS companies in Europe.

Other vectors. Crowdstrike's (2013) research determined the SWC tactic was the preferred exploit used by Energetic Bear; but they also created exploits for exploits for popular document readers, e.g., Adobe Reader.

RATS might also be inserted through compromise of the supply chain. This could entail contamination of firmware on equipment, such as a printer's driver. It might also be characterized by a witting or unwitting human attack – adding the malware to a thumb drive used at work – though this was not indicated, or at least detected, in the Energetic Bear HAVEX RAT attack profiles.

During the HAVEX campaign the following sites were positively identified as SWCs: (Crowdstrike, 2014, pp. 4-6). *Figure 5- More HAVEX SWCs*

- The Council on Foreign Relations (cfr.com)
- Capstone Turbine (capstonturbine.com)
- Napteh Engineering & Development Company (naedco.com)
- DFG (instrumentenkasten.dfg.de)

• Uygur Haber Ajansi (uygurunsesi.com)

• Quick Fire (quick-fire.com) (Crowdsp. 6).

Signatures. Forensic exploitation of HAVEX by the malware laboratory F-secure (2014), found the word HAVEX within the servers' source code. This code was written in the PHP programming language. *Figure 4- HAVEX code*

HAVEX was not intended only to exfiltrate data, but to enable actual control over the affected ICS, though the end purpose was not clear. Using Windows OLE for Process Control, or OPC, HAVEX also gathered information on all connected devices and returned it to the malware operators in Russia (Hentunen, 2014). While no actual control actions were taken against connected devices, this is an obvious intelligence gathering function of the malware.

Intelligence Analysis against HAVEX

Who was the target? The two apparent biggest players in the HAVEX malware case, Symantic and Crowdstrike, seem to agree on the energy sector as the intended target, as does much of the follow-on reporting and observation by other organizations (Symantec, 2014) (Crowdstrike, 2014). An interesting minority opinion (cf. Langill, 2014) appeared late in October, 2014. According to a 2014 white paper published by cyber security firm Belden, an ICS Cyber Security Expert with a background in pharmaceuticals, J. Langill, identified the pharmaceutical industry as the actual target. Though several of the vendors targeted in the SWC were indeed ICS providers, author Langill deduced that they were ICS providers for the pharma industry.

Link analysis demonstrated a large number of pharma critical nodes throughout the intelligence gathering facets of HAVEX as well as end-SCADA control attacks. The list of known victims also focused on machine, packaging, and pharmaceutical products.

When academic targets were removed from the victim list of 101 organizations, and the list was analyzed for machine, packaging, and pharma links, these predominated. With HAVEX having a dual purpose of intelligence gathering and preparing for execution of unauthorized commands to SCADA, damage could include intellectual property such as formulations, production steps, and information about the devices on the network, what they control, and details about production volumes and capabilities (Langill, 2014).

CONCLUSION

HAVEX utilized an aggressive network attack and reconnaissance capability. Careful social engineering, target analysis, and application were used in attacks upon hundreds of organizations from 2010 and continuing in a diminished volume today.

HAVEX was studied from many angles by preeminent network protection companies. Although given different names by different analysts, all are in agreement on one fact; the threat originated in Russia. Although not implicitly stated in each case it is clear that an effort of this magnitude, accomplished with regular business hours from a centralized location, is most likely either government sponsored or government executed.

The cyber domain is recognized as an operational domain by the United States, Russia, and many other countries. If we consider HAVEX to be an intelligence gathering tool then we must consider its purpose may be intelligence preparation of the battlefield, a necessary precursor to the execution of any well organized campaign. In the absence of military conflict, economic espionage is also a strong possibility.

It is also possible to visualize the following scenarios: after infiltration and reconnaissance of pharmaceutical production targets in the United States, proprietary and intellectual property is exfiltrated to the Russian government, who takes advantage of the

information to reduce the research cycle for the production of modern drugs. The same information might also be sold to a third-party who will use it for economic gain, e.g., China.

A more serious consideration is the intent of the threat actor with regards to the SCADA controls. Were in adversary to maintain a SCADA override ability with regard to these pharmaceutical companies and their production technology it would be a simple matter to disable the entire manufacturing line. Taking this possibility one step further and incorporating Russian backing, such an action would be a very effective precursor to a biological attack. Without the ability to manufacture vaccines, prophylaxis, and treatments, even common and controllable ailments such as diabetes become deadly. Were this to occur prior to a biological attack, or even in case of national medical emergency such as the current Ebola threat, the force multiplier effect created by such a combined attack could cause nationwide disaster.

REFERENCES

Bailey, E. W. (2003). *Practical SCADA for Industry.* Boston: Elsevier.

Boyer, S. A. (2009). *SCADA: Supervisory Control and Data Acquisition.* International Society of Automation.

Crowdstrike. (2014, January). *Crowdstrike Global Threat Report 2013 Year in Review.* Retrieved from SCADAhacker.com: http://scadahacker.com/library/Documents/Threat_Intelligence/CrowdStrike%20-%20Global%20Threat%20Report%202013.pdf

Definition: Remote Access Trojan. (2012). *Security Search Index*. http://searchsecurity.techtarget.com/.

Hentunen, D. (2014, June Monday). *Havex Hunts For ICS/SCADA Systems*. Retrieved from f-secure.com: https://www.f-secure.com/weblog/archives/00002718.html

Herbert J. Mattord, M. E. (2011). *Principles of Information Security.* Boston, Massachussetts, US: Course Technology Press.

Hjelmvik, E. (2014, October 27). *Full Disclosure of Havex Trojans.* Retrieved from netresec.com: http://www.netresec.com/?month=2014-10&page=Blog&post=Full-Disclosure-of-Havex-Trojans

Kovacs, E. (2014, June 24). *Attackers Using Havex RAT Against Industrial Control Systems*. Retrieved November 16, 2014, from SecurityWeek.Com: http://www.securityweek.com/attackers-using-havex-rat-against-industrial-control-systems

Langill, J. T. (2014). *Defending Against the Dragonfly Cyber Security Attacks.* redhatcyber.com. Belden. Retrieved November 30, 2014, from http://www.belden.com/docs/upload/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks.pdf

Marschalek, M. (2014, June 30). *Windows meets industrial control systems (ICS) through HAVEX.RAT – It spells security risks.* Retrieved from Cyphort.com: http://www.cyphort.com/windows-meets-industrial-control-systems-ics-havex-rat-spells-security-risks-2/

McAfee. (2011). *Combating Advanced Persistent Threats.* Santa Clara: McAfee.

Paganini, P. (2014, June 25). *Cyber espionage campaign based on Havex RAT hit ICS/SCADA systems*. Retrieved from Security Affairs: http://securityaffairs.co/wordpress/26092/cyber-crime/cyber-espionage-havex.html

Paganini, P. (2014, November 25). *The looming cyberthreat to America's backbone*. Retrieved from foxnews.com: http://www.foxnews.com/tech/2014/11/25/looming-cyberthreat-to-americas-backbone/

Rodillas, D. (2014, July 17). *Why Havex Is a Game-Changing Threat to Industrial Control Systems – Parts 1&2.* Retrieved from http://researchcenter.paloaltonetworks.com/: http://researchcenter.paloaltonetworks.com/2014/07/havex-game-changing-threat-industrial-control-systems-part-1/

Symantec. (2011). *Advanced persistent Threats: A Symantec Perspective.* Mountain View: Symantec Corporatoin.

Symantec. (2014, June 30). *Emerging Threat: Dragonfly / Energetic Bear.* Retrieved from Symantec.com: http://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group

TABLE OF FIGURES

Figures

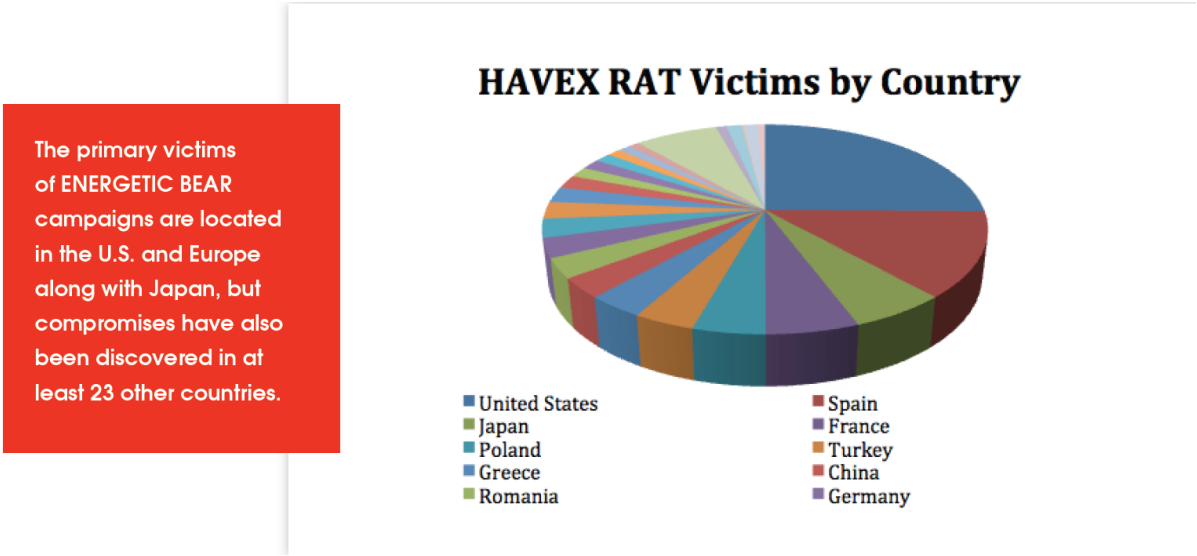

Figure 1- HAVEX RAT by country (Crowdstrike, 2014)

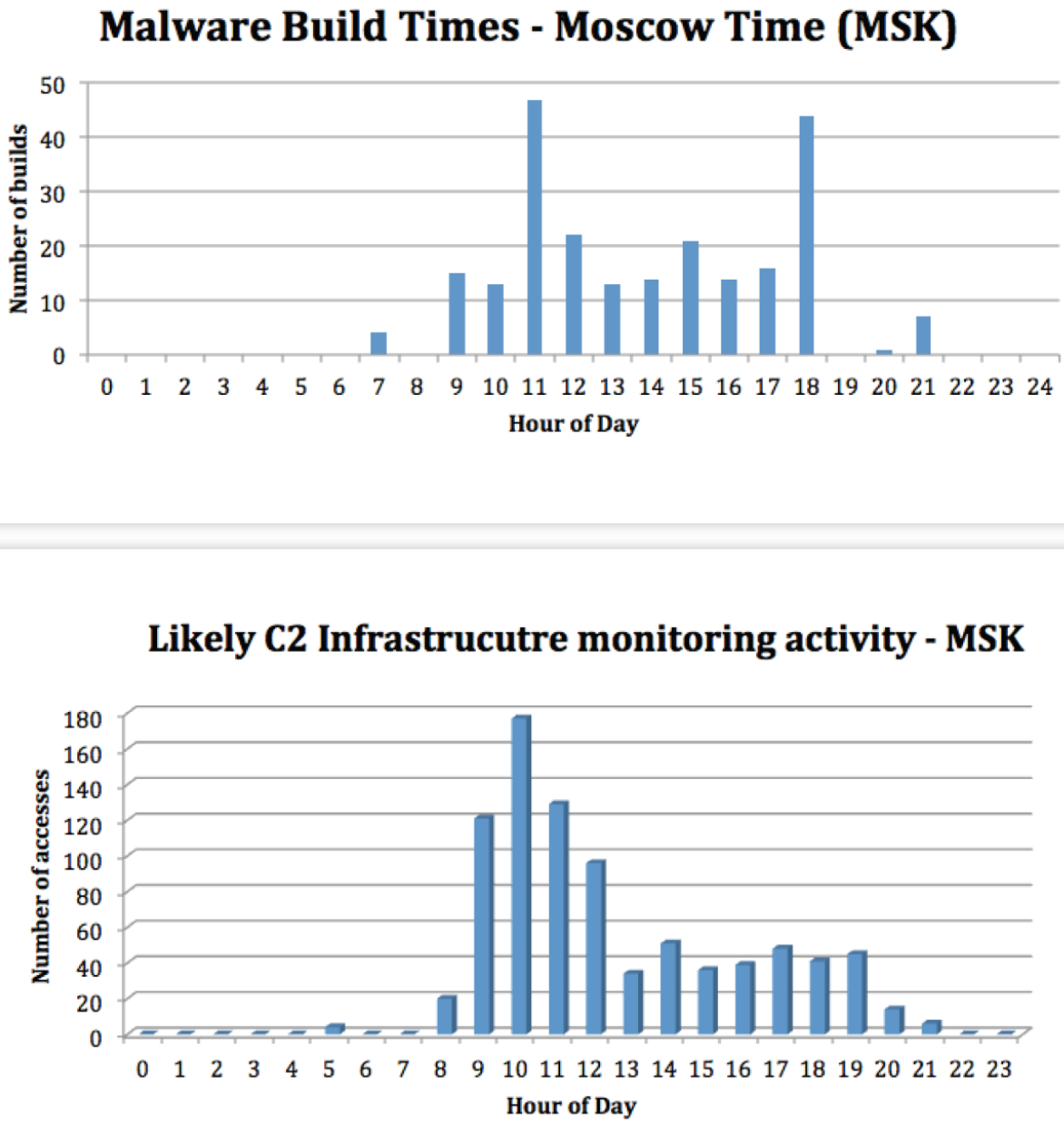

Figure 2- Forensic timestamp evidence (Symantec, 2013)

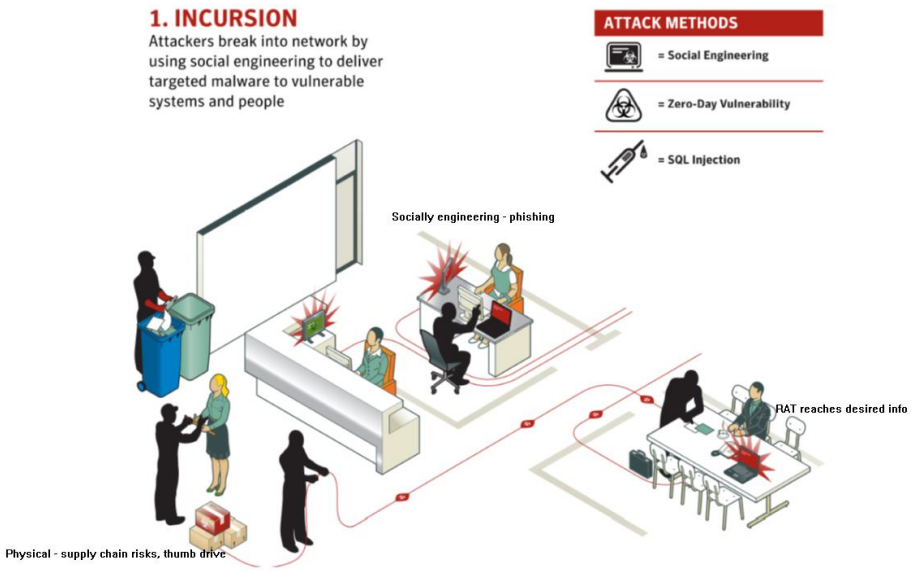

Figure 3- HAVEX RAT penetration (Symantec, 2011)

```
define("PATH_BLOCKFILE", "block.tmp");
define("PATH_LOGFILE", "testlog.php");
define("DATATAG_START", "<html><head><mega http-equiv='CACHE-CONTROL' "
       "content='NO-CACHE'></head><body>No data!<!--havex");
define("DATATAG_END", "havex--></body></head>");
define("NODATA", "<html><head><mega http-equiv='CACHE-CONTROL' "
       "content='NO-CACHE'></head><body>Sorry, no data corresponding your request."
       "<!--havexhavex--></body></html>");
define("ANSWERTAG_START", "<xdata d='%s' u='%s'>");
define("ANSWERTAG_END", "</xdata>\n");
define("FILE_OUTPUT_BLOCK_SIZE", 16384);
```

Figure 4- HAVEX code (Hjelmvik, 2014)

```
abainternationaltoursandtravel.com
adultfriendgermany.com
africancranesafaris.com
alexvernigor.com
al-mashkoor.com
alpikaclub.com
antibioticsdrugstore.com
arsch-anus.com
artem.sataev.com
artsepid.com
ask.az
atampy.com
aziaone.com
```

Figure 5- More HAVEX SWCs[2] (Hjelmvik, 2014)

[2] If my German is still good, anybody who went to that eighth site probably deserved it.