TECHNICAL CIRCULAR No. 487 of 05th June 2018

To:	All Surveyors/Auditors
Applicable to flag:	All Flags
	The Seven Phases of a Cyber Attack
Reference:	Cyber Security

The Seven Phases of a Cyber Attack

In the cyber security industry, we are seeing a change in the way that hacks are being performed. A recent set of attacks against critical infrastructure entities, such as oil and gas pipeline operators, utilities and even some city and state governments reveal new motives and methods. The attackers were not out to steal data but were looking to disrupt services. The attackers used a new attack vector that has not been seen before. Instead of attacking their primary targets directly, they attacked less secure vendors that those targets use.

Step one - Reconnaissance

Before launching an attack, hackers first identify a vulnerable target and explore the best ways to exploit it. The initial target can be anyone in an organization. The attackers simply need a single point of entrance to get started. Targeted phishing emails are common in this step, as an effective method of distributing malware.

The whole point of this phase is getting to know the target.

The questions that hackers are answering at this stage are:

- Who are the important people in the company? This can be answered by looking at the company web site or LinkedIn.
- Who do they do business with? For this, they may be able to use social engineering, by make a few “sales calls” to the company. The other way is good old-fashioned dumpster diving.

Customer Service Center
5201 Blue Lagoon Drive, 9TH. Floor,
Miami, Fl., 33126
Tel: 1 (305) 716 4116,
Fax: 1 (305) 716 4117,
E-Mail:
joel@conarinagroup.com

Technical Head Office
7111 Dekadine Ct.
Spring, Tx., 77379
Tel: 1 (832) 451 0185,
1 (713) 204 6380
E-Mail: vbozenovici@vcmaritime.com

• What public data is available about the company? Hackers collect IP address information and run scans to determine what hardware and software they are using. They check the ICAAN web registry database.

The more time hackers spend gaining information about the people and systems at the company, the more successful the hacking attempt will be.

Step two - Weaponization

In this phase, the hacker uses the information that they gathered in the previous phase to create the things they will need to get into the network. This could be creating believable Spear Phishing e-mails. These would look like e-mails that they could potentially receive from a known vendor or other business contact.

The next is creating Watering Holes, or fake web pages. These web pages will look identical to a vendor's web page or even a bank's web page. However, the sole purpose is to capture your user name and password, or to offer you a free download of a document or something else of interest.

The final thing the attacker will do in this stage is to collect the tools that they plan to use once they gain access to the network so that they can successfully exploit any vulnerabilities that they find.

Step three - Delivery

Now the attack starts. Phishing e-mails are sent, Watering Hole web pages are posted to the Internet and the attacker waits for all the data they need to start rolling in. If the Phishing e-mail contains a weaponized attachment, then the attacker waits for someone to open the attachment and for the malware to call home.

Step four - Exploitation

Now the "fun" begins for the hacker. As user names and passwords arrive, the hacker tries them against web-based e-mail systems or VPN connections to the company network. If malware-laced attachments were sent, then the attacker remotely accesses the infected computers. The attacker explores the network and gains a better idea of the traffic flow on the network, what systems are connected to the network and how they can be exploited.

Step five - Installation

In this phase the attacker makes sure that they continue to have access to the network. They will install a persistent backdoor, create Admin accounts on the network, disable firewall rules and perhaps even activate remote desktop access on servers and other systems on the network. The intent at this point is to make sure that the attacker can stay in the system as long as they need to.

Customer Service Center
5201 Blue Lagoon Drive, 9TH. Floor,
Miami, Fl., 33126
Tel: 1 (305) 716 4116,
Fax: 1 (305) 716 4117,
E-Mail:
joel@conarinagroup.com

Technical Head Office
7111 Dekadine Ct.
Spring, Tx., 77379
Tel: 1 (832) 451 0185,
1 (713) 204 6380
E-Mail: vbozenovici@vcmaritime.com

Step six – Command and control

Now they have access to the network, administrator accounts, all the needed tools are in place. They now have unfettered access to the entire network. They can look at anything, impersonate any user on the network, and even send e-mails from the CEO to all employees. At this point they are in control. They can lock you out of your entire network if they want to.

Step seven – Action on objective

Now that they have total control, they can achieve their objectives. This could be stealing information on employees, customers, product designs, etc. or they can start messing with the operations of the company. Remember, not all hackers are after monetizable data, some are out to just mess things up. If you take online orders, they could shut down your order-taking system or delete orders from the system. They could even create orders and have them shipped to your customers.

If you have an Industrial Control System and they gain access to it, they could shut down equipment, enter new set points, and disable alarms. Not all hackers want to steal your money, sell your information or post your incriminating e-mails on WikiLeaks, some hackers just want to cause you pain.

REFERENCES:

- Cyber Security -**Craig Reeds**

- ATTACHMENTS: No.

Kindest Regards,

Val Bozenovici
Naval Architect – Conarina Technical Director

Customer Service Center
5201 Blue Lagoon Drive, 9TH. Floor,
Miami, Fl., 33126
Tel: 1 (305) 716 4116,
Fax: 1 (305) 716 4117,
E-Mail:
joel@conarinagroup.com

Technical Head Office
7111 Dekadine Ct.
Spring, Tx., 77379
Tel: 1 (832) 451 0185,
1 (713) 204 6380
E-Mail: *vbozenovici@vcmaritime.com*