Are you ready to handle a network security breach?

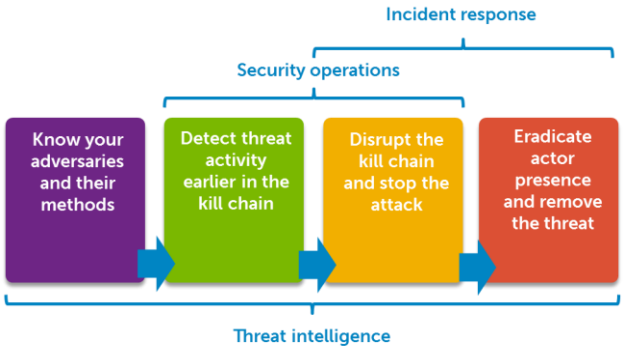
By Col. Jeff Schilling

The targeted cyber threat, commonly referred as the Advanced Persistent Threat (APT), is coming to a network near you soon, if it is not already there. Well-funded by nation-states and criminal gangs, APT actors have near unlimited time and resources. Because the United States is still the world's largest and most prosperous economy, the threat actors behind APTs are trying to close gap between their nation-state's businesses and those in the U.S. These actors steal your organization's intellectual property and sell goods and services similar to or exactly like yours to companies and individuals around the world at lower prices, putting your company at financial risk and customer loss. If you have cutting-edge intellectual property or financial information that can be leveraged for advantage in international commerce, you most likely will be targeted, and your network may have already been breached, and you may not even know it.

So, you've got to know the best way to mitigate a breach immediately and the best way to avoid a breach altogether. Your best defense against a breach is to have a tightly integrated approach among your cyber threat intelligence, security operations and incident response teams to narrow the surface area of your network that is vulnerable to attack. This team integration will allow you to detect the threat actor presence rapidly and then slam the door shut before the attacker can do any damage or steal any intellectual property.

There are four major functions required to protect a network from attack: 1) Know what adversary activity to look for on your network. 2) Detect the adversary activity. 3) Disrupt the adversary from gaining information and expanding a foothold in your network. 4) Eradicate the adversary from your network.

Each of these activities is supported by three tightly integrated components: cyber intelligence, security operations and incident response.



Threat intelligence is a critical component of cyber security. Threat intelligence is the knowledge one has about threat actors and the digital trails they leave behind. Knowing the tools, techniques and procedures they use, helps you know how to block them and find malware they may have already

hidden inside your network. Threat intelligence provides the "threat" variable in the risk equation (Risk = Threat + Vulnerability). Once your threat intelligence team identifies signs of possible adversaries in your network, it should tell your security operations team what signs of activities and what patterns they should be looking for on your network. Once these breach indicators have been detected on your network, your threat intelligence team should continue to inform both your security operations and your incident response teams on ways to disrupt the threat activity to stop the attackers from expanding their foothold on your network. Your forensics team should then analyze the malware and look for any documents that may be hiding Trojans or "backdoors," which could allow a hacker to access devices on your network. Breach indicators could include domains, Internet addresses, ports and protocols that are used to communicate with the threat actors. Once you know these breach indicators, you can tune your network defenses to find all of the infected machines on your network.

Finally, threat intelligence is critical to ensuring the threat is completely eradicated from your networks. One thing you can count on with a targeted threat: the attackers will attempt to regain access to your network once you have eradicated them. Remember, the "P" in APT stands for "persistent." Your threat intelligence should help you anticipate this re-attack and should inform your security operations team how to stop and/or detect this threat activity.

Your threat intelligence team must be knowledgeable about adversary activity on networks other than the ones it is trying to protect. For example, an aviation manufacturing company should have threat intelligence on network attacks on other aviation manufacturing companies. Having a global view of activity occurring on similar types of manufacturing companies allows the aviation company to know what types of threats are ahead for them. That knowledge helps your organization block threats and find them in the event an attacker gets into the network. If your threat intelligence is based only on activity on your network, your security operations team will only be able to operate in reactive mode. It won't be able to proactively prepare and protect your network from vectors that can be seen on other networks outside of your own. If you rely only on an internal intelligence research team, you likely won't have the resources to conduct global threat intelligence work. That is why working with an information security company with global threat intelligence is so important.

The next critical component to protecting your networks is having a top-notch security operations team. Your security operations team manages security controls you have in place to protect your networks, to prevent breaches and to detect breach indicators. These activities include managing your boundary defenses (your intrusion protection systems and firewalls), monitoring your security event logs from critical systems such as the Active Directory and critical applications servers, and observing known vulnerabilities on your network or in applications like Adobe, Oracle and Microsoft Office. Your security team should base its operations on looking for signatures that are known as harmful and on looking for abnormal activity. Based on global threat intelligence, your security team should tune and monitor your security controls to ensure you stop and/or detect a breach when it occurs. Some organizations believe that if they have a Security Information Event Manager (SIEM) in place, they are conducting security operations. For most medium to large enterprises, these security events could number in the millions per day. It is not enough to see all the security alerts on you network; you need data analytics to inform you which alerts are the ones that should drive you immediately to incident response.

Once you have detected a possible breach, take action immediately with incident response. The quicker you contain a breach, the less damage to your network. The first action begins with taking out your Computer Security Incident Response Plan (CSIRP). Every company should have a CSIRP that is rehearsed and updated annually. Most regulated industries (i.e. HIPPA, SOX) require an organization to have a CSIRP in place. The CSIRP should be comprehensive and guide an organization through the following: 1) discovery of a breach, 2) declaration of an incident, 3) analysis of what happened, 5) containment of the breach, and 6) eradication of the threat and return to normal operations.

The discovery of a breach never happens the same way. However, there are common attributes to look for in a security incident that would alert your staff that you may have been breached. Some signs are obvious, like having an FBI agent show up at your doorstep to inform you that you have a breach. If that happens, go to step two as soon as the agent presents his or her badge. Other breach indicators are more subtle and require the incident management team to assess whether a breach has occurred. An example of a more subtle breach indicator could be a recurring malware outbreak that just keeps coming back to you, and your staff can't stop it from returning. Another example could be seeing unexplained or unauthorized administrator activity, especially around Domain Controllers and other network infrastructure. When a breach is suspected, the Security and IT staff should assess what they know and don't know about the incident to put as many pieces of the puzzle together before they declare a breach. Once they have all the facts, they should consult the CSIRP, which should clearly explain the criteria for declaring a breach.

Once your security team declares there has been a breach, it should inform the incident management team, and it should assemble within minutes. The incident management team should consist of both the security and IT service delivery team members, as well as members on teams from the company's affected business owners, legal staff and public relations.

An incident manager should take charge of the team and start the analysis phase of the breach. This requires highly specialized skills that most organizations do not maintain on their security or IT staffs. At this point in the breach, you must be able to conduct network forensics, systems forensics and malware analysis to determine the extent of the foothold the APT has on your network. By reviewing network and security event logs, a forensic analyst can determine which computer systems are likely compromised. Once an infected system is recovered for analysis, the forensics analysts will examine the system to retrieve the files that are responsible for the threat activity. These files are normally hiding some type of Trojan or back door. The forensic analyst will then conduct deep malware analysis on the captured files that make up the Trojan to determine what the malware does and how it communicates back to the APT actors. There are normally distinctive Internet addresses, network protocols, processes and other signatures that are unique to targeted malware. These unique signatures or activities are referred to as threat indicators. Once the forensic analyst discovers the threat indicators, your security experts can determine new security controls to counter the APT actor's foothold. Once your new security controls are determined, your security experts can develop the containment plan.

The containment plan is the most important phase of breach. Your objective in containment is to slam the door shut on the threat actor's access to your network. Timing is critical for the containment plan.

All of the security controls to counter the threat's access must be implemented within minutes so the threat has no time to react. This requires precision coordination between the IT staff, security team and business owners. The threat actor must not suspect you are about to conduct containment. Limit communications about the plan, especially over email, so you don't tip the APT actors about your plan as they probably are accessing your emails. Most of the coordination should take place, face to face or over the telephone unless you suspect your telephones have also been compromised. During this phase, you will update antivirus and intrusion protection signatures, change firewall rules, and block communications with the Internet addresses of the suspected "bad guy." When your IR team implements the CISRP with speed and precision, the threat actor will lose his or her foothold on your network. If your containment plan is executed successfully, you can expect the threat actor to conduct a re-attack though spear phishing or website compromises to regain the foothold. Your containment plan should position you to be ready for this re-attack through additional security controls and/or email and website filtering technologies.

Once you break the APT actors' communications with their foothold on your network, you can eradicate their presence. During the containment phase, your security team should have identified the breach indicators to look for on your network to determine all of the infected systems. Once all of the infected systems have been identified, the IT staff will usually wipe and reimage most machines unless the incident management team decides it can conduct forensics on all infected hosts. This is sometimes required if a company has regulatory requirements to report breaches. At this point, the team should conduct a data loss assessment on all of the systems that have files that may be at risk and require notification. These files include those that contain Personal Identification Information and Payment Card Industry information.

After the eradication phase has been completed and all systems have returned to normal operations, the incident manager should conduct a post incident review to determine the root cause of the breach make suggested changes to the CSIRP to reflect lessons learned.

We're all going to have that bad day when we discover we have been breached. No matter how good your cyber intelligence and network security program is, eventually the targeted threat will find a weakness. The targeted threat will find that one person who will click on a spear phishing email or that one server that you have not gotten around to patching, or that zero-day exploit that you had no idea was a problem. You must be ready to respond quickly and decisively to stop the threat to keep the threat actors from expanding their foothold on your network, and to limit the exposure of your critical data and intellectual property. A tightly integrated approach to threat intelligence, security operations and incident response will give you the best chance to detect and respond to a breach quickly before any real damage occurs.

Retired Col. Jeff Schilling, a former director of the Army's Global Network Operations and Security Center (AGNOSC) under the U.S. Army Cyber Command, is the director of the Incident Response Practice at Dell SecureWorks. Contact him at Jeff@Secureworks.com.