The Anatomy of an Advanced Persistent Threat

By Terry Cutler on Dec 06, 2010

What is an Advanced Persistent Threat? Attackers are Getting More Sophisticated - Here's an Example of How they Work and Insight on How to Stop Them.

The news just broke: Acme has completed a strategic acquisition of Landmark and both companies are being tight-lipped concerning all of the details. Should the acquisition proceed, that's bad news for Acme's toughest competitor, which would – as a result of the deal – be set to lose a clear market advantage.

That competitor is going to do what many do today when they need information. It's going to steal it electronically. It has contracted a black hat hacker, and that hired hacker now has three objectives: find as much information about the Landmark acquisition as possible; steal as much competitive information as possible; and, of course: do not get caught.

First up for our nefarious attacker: find a target that will provide entry into Acme's IT systems. Thanks to the magic of social networking sites such as Twitter, Facebook, LinkedIn and others, that task is easier now than ever. So, our attacker starts to troll online hangouts looking for anyone and any information that could be useful.

Fortunately, or unfortunately for Acme, a few searches on LinkedIn turned up Keith, a security analyst at Acme. Keith likes to Tweet. A lot. And he's been blabbering about his day at home with the kids after his return from Black Hat, the movies he intends to watch this weekend, and his excitement over the Landmark acquisition.

The Attack Acme Can't Stop

This sets up the hacker's first approach in his mission. A familiar social engineering ploy that leverages the information Keith tweeted about himself: "Hi Keith, it was great meeting you at Black Hat. I'd like to add you as a member of my LinkedIn network," is all the note needed to say.

Only that wasn't an authentic LinkedIn e-mail; rather it was a specially crafted e-mail. And when Keith clicked on the bogus LinkedIn invitation, a malware application was installed on his PC that gives the hacker full access to his workstation as well as his network credentials. Unfortunately, Keith doesn't know this, but the attacker now is using his access to attack the network he's supposed to help keep secure.

So now our attacker, with his newfound foothold, can unleash the full power of his arsenal and work to find any information about the Landmark acquisition, and any other competitive information that may be of use:

- He can take screenshots of the compromised workstation to make sure the malware has been deployed successfully on his target.
- He can retrieve stored passwords from the browser for later use.

Most Read | Most Recent

- Survey Reveals How Stupid People are With Their Passwords
- New Tool Reveals Internet Passwords
- Hacker Uses XSS and Google Street View Data to Determine Physical Location
- Snoop Dogg Joins the War on Cybercrime
- Study Reveals 75 Percent of Individuals Use Same Password for Social Networking and Email
- The Rise of the Small Botnet
- An Inside Look at Hacker Business Models
- IT Salary Guide Shows Increase in Salaries for IT Security Professionals
- Defense Department's Cyberwar Credibility Gap
- Nevercookie Eats Evercookie With New Firefox Plugin
- Veracode Expands Mobile App Verification Service to Android and iOS
- IBM Launches Initiatives to Help Secure the Exploding World of Connected Devices
- Sourcefire Unveils Immunet 3.0 with Ability to Create Custom Anti-Malware Signatures

• He can run a software inventory to find out all the applications on the compromised machine.

• He can install a key logger and network sniffer to capture passwords and other activity from the user, then come back later to retrieve them.

After all of that fun, our attacker now rummages through Keith's current contact lists, making note of a few VIPs. He captures Keith's current encrypted username and password and he now can pass these stolen credentials directly to additional servers and get immediate access, without even needing to decrypt or crack the password. And with that exact goal in mind, the attacker then opens a shell prompt to Keith's computer to try to discover if his computer is mapped to a network drive.

Fortunately for the attacker, Keith's system currently is connected to the network drive. That fact calls for a port scan from Keith's system. By doing this, the attacker will identify available ports, running system services on systems, and he'll spot network segments. With a network map now in place, the attacker goes back to one of the VIPs he previously took note of within Keith's contact list: Norman Devries, ACME CEO. Devries would have access to the acquisition data for sure. And our attacker needs to do nothing more than he did before. And that's to send an email to the CEO which would appear to come from his trusted IT administrator Keith asking him to apply a patch. Once the CEO clicks, the deed is complete, the attacker has access to the Landmark acquisition details ($53 million), product integration plans, new services to be launched as a result of the acquisition, and a number of other corporate secrets. He is able to do this because he was able to piggyback off of Norman's authentication credentials.

Rising APT Threats

Until recently, attacks like the one we just described in our fictional example would have been considered as exceptional or rare. Not anymore. Consider the Operation Aurora attacks, which employed some of the tactics we touched on above. The Operation Aurora attacks targeted many companies, in addition to Google, such as Adobe Systems, Juniper Networks, Rackspace, Yahoo, Symantec, Northrop Gruman and Dow Chemical.

Interestingly, the vast majority of attacks reveal that enterprises have the data on hand to stop, or at least mitigate, the risk long before most hacker breaches are uncovered. Consider the 2010 Data Breach Investigations Report from Verizon Business: It found that while 86 percent of data breach victims had evidence of the breach in their audit logs, 61 percent of those victims didn't uncover the breach themselves – they were notified by a third party. How embarrassing.

Defending Against the Modern Attackers

How do you put all of that data in your audit logs to work? And more importantly, how do you stop attacks like the one that befell Acme? First: Make sure that you capture the data that could detail security events on your network. You probably have more security data than you realize scattered throughout firewall, application, router, and other log sources. Most enterprises have an enormous amount of data that is useful for determining what sorts of things are going on within their networks. The trouble is that they don't know how to aggregate and put that data to actionable use.

That brings us to my next point. You need to put into place the processes and possibly the technology necessary to cultivate your security logs and pinpoint the information needed to keep the infrastructure secure. Those efforts absolutely require some type of log management. Even better would be the installation of a Security Information Event Manager (SIEM) to capture and correlate that data. It's also crucial to take that one step further and integrate that data with identity and access information. That way, in our hacking example, a number of alerts would have been fired off to security managers long before any of your proprietary data was accessed.

While you read about how security threats have grown more menacing, it's important to also remember that security defenses also have grown more powerful. The critical thing is to take the necessary steps to protect your infrastructure and your data. That's where most businesses fall short. And it's a mistake that is growing increasingly costly to make.

Terry Cutler is a co-founder of Digital Locksmiths, Inc., an IT security and

Previous Columns by Terry Cutler:

- VASCO's DIGIPASS Technology to be Embedded Into Intel Identity Protection Technology
- 'Internet Kill Switch' - Is this Technically Feasible in the US?
- Organizations Struggle with Data and Application Security Budgets & Strategies
- Dell Completes Acquisition of SecureWorks
- Agiliance Launches Cloud-Based PCI Compliance Service
- One in Three Experience Mobile Device Loss or Theft. Do People in 'Party Cities' Lose More Phones?
- Mobile Threats Trending Upward, More Connected Devices Mean More Threats

data defense firm based in Montreal and serves as the company's Chief Security Evangelist and Certified Ethical Hacker. Prior to joining Digital Locksmiths, he was a Premium Support Engineer for Novell in Canada where he analyzed network vulnerabilities and transitioned security technologies into production. In addition to being a licensed private investigator in Canada, Terry is an internationally known author, trainer, speaker, and security consultant, Terry has appeared in numerous national television and radio programs and is very active on the conference circuit. Follow Terry on Twitter at @TerryPCutler

Beating Back the Botnets

» Enterprise Security Priorities for 2011

» Mobile Security: It's Time to Get Serious

» The Anatomy of an Advanced Persistent Threat

Tags: INDUSTRY INSIGHTS Virus & Threats Incident Management Risk Management Cybercrime

Showing 0 comments

Sort by Best rating **Subscribe by email** **Subscribe by RSS**

Add New Comment

Type your comment here.

Post as ...

Trackback URL http://disqus.com/forums/securityweek/anator