LIGHTCYBER

CLOSING THE BREACH DETECTION GAP

# FIVE WAYS TO FIND AN ATTACKER IN YOUR NETWORK

REPORT / MAY 2016

## Five Ways to Spot an Attacker in Your Network

We all know the attackers are getting in. The only question that remains is how to find them – fast! The good news is that an attack doesn't end with infection or take-over of an endpoint; that is where it begins. From there an attack is highly active, and the attacker can be identified and stopped if you know how to look. Here are some key things to look for to spot attackers:

### 1 Look for an attacker trying to learn your network topology (port scans).

An attacker will initially need to map the network environment in which they find themselves. See if you can get a sense for how many ports and destinations different devices on your network usually access, and look for outliers.

> Data Source: network monitoring or management tools, netflow aggregation

> Challenges: Attackers can go "low and slow" though, so you may need to do some time based analysis. Also, there can be a lot of chatty tools and protocols, so it takes a while to filter out the noise.

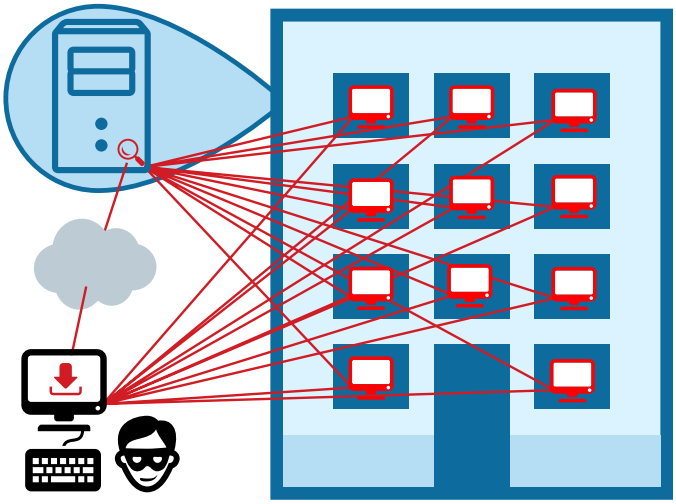

Figure 1: Where am I and What else is here?

### 2 Look for an attacker trying to find data (recon of file shares).

An early step an attacker (or networked ransomware) will take is to figure out what Windows files shares are broadly accessible in order to either hunt for valuable data, or to remotely encrypt for ransom. Spotting anomalies in file share access can be a valuable signal, and may also alert you to an employee who is considering insider theft.

> Data Source: logs from your file servers are the best bet to do this yourself. But it will take some analysis to turn this into a view from the users' perspective, and thus grant the ability to see user-access anomalies

> Challenges: Some file shares are truly commonly accessed, and a large spike as a user goes there for the first time might generate a false positive. In addition, the data on access is pretty messy and hard to analyze. This can be seen with network tools as well, but it is a lot of work to extract the information that matters.

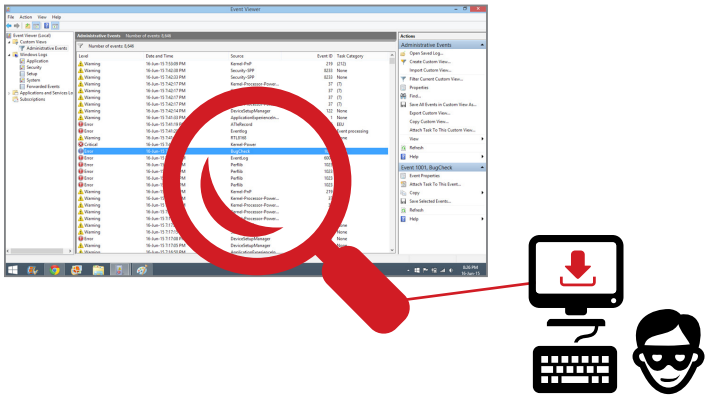

Figure 2: Where is the pay data?

## 3 Look for an attacker trying to extend their control (lateral movement - new admin behavior).

Increasingly attackers are "living off the land," meaning using less malware and more admin tools and protocols to avoid detection by anti-virus and EDR agents. But, this is itself an anomaly you can look out for. Try to determine who your admins are (AD or other user tools can help), as well as which users are using admin-like functions (SSH, or admin access via HTTP to /admin url's, etc.). With that baseline, you can spot when an attacker takes over a machine and starts using sophisticated tools.

> Data Source: combination of network information (netflow if you must) and directory information gives you your best bet.

> Challenge: this is a tough one- there isn't a great single source of information, but even just monitoring SSH and RPC usage from a course perspective can give you a good starting point. You'll probably end up with a lot of false positives, but over time you can winnow down the list of approved/expected admins, and from that have a baseline you can detect against.


Figure 3: What systems can I control?

## 4 Look for an attacker flexing their muscles (excessive credential usage).

Attackers love credentials. They steal or generate accounts and use those to explore and gain access. This is a mark of both external and internal attackers. Analyze credential usage to spot outliers that are indicative of such attack activity.

> Data Source: logs from your authentication/authorization infrastructure are probably your best bet. Extract the data and analyze it to get a sense for how many systems each user generally interacts with. Then monitor for anomalies.

> Challenges: there is a lot of variability in users, so you can do this as a single baseline for the "average" user. But even just listing out your high volume users should give decent visibility- if you see a new name pop onto the list you can check it out.


Figure 4: What systems can I own?

## 5 Look for the phone-home and persistent access mechanisms (command & control).

Attackers need a way to communicate between the Internet and endpoint(s) they control in your environment. While there is less malware in use throughout the attack than there used to be, there can still be malware and RATs in place. Keep an eye on outbound communications for indications of malware phoning home.

> Data Source: many of your perimeter tools are likely already doing this, but you can augment it by looking at DNS logs for patterns of look-ups that indicate malware trying to hide from blacklists. Lots of requests that fail and look like machine-generated names are a sign of malware programmed to avoid reputation based blocking.

> Challenges: Attackers have a lot of ways of concealing this traffic, so it is good to keep an eye out, but don't rely on C&C detection alone – you can never tell what combination of normal Internet services may be at use (twitter + craigslist + HTTP posts + who knows what). Also, many of your tools are probably already looking for C&C. So, it is worth spending some time here, but isn't as important as some of the other steps (above) that are fundamentally much more difficult for an attacker to conceal.

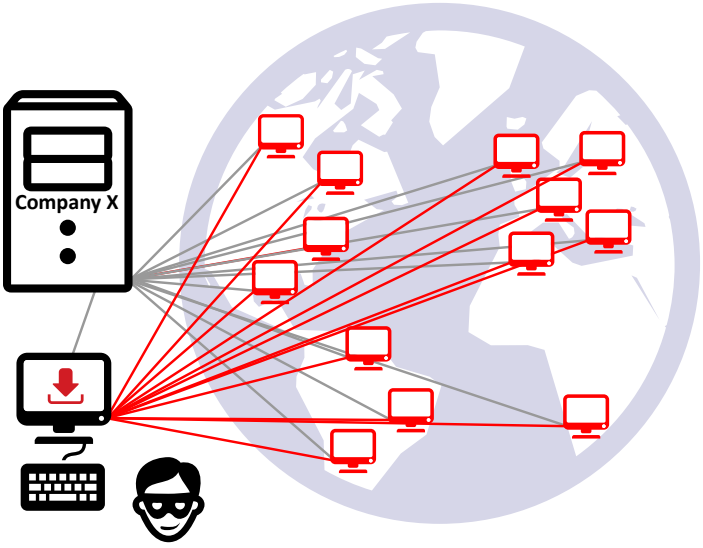


Figure 5: How do I phone home?

## In Conclusion

As you can see, there are a lot of tools at your disposal to help spot attackers. There are many activities they must engage in to learn and expand in an environment. Getting in, for them, is just the first step. At a minimum, a bot needs to connect back and monetize somehow (bitcoin mining, click fraud, spam, etc.), In the more serious cases, the initial intrusion is just the beachhead the attacker uses to then learn and expand on your network in the pursuit of your data. In either case, all is not lost upon intrusion- there is still plenty of time to find and root out attackers and malware before serious damage is done.

Further, it is actually possible to spot all these activities, and more, directly from the network- if you are able to extract the right metadata from the packet flows. This is harder to do manually, but is a great option for an automated tool, which is why it is the approach taken by LightCyber Magna. Whether manual or automated, the above is a good starting point and can be taken much further, both on your own, or by partnering with LightCyber.

If you are interested in automating these detection steps and more – LightCyber Magna™ has dozens of additional attack detectors, and uses machine learning to automate the baselining process on your network so you can quickly find and stop attackers who have circumvented traditional prevention controls.

## About LightCyber

LightCyber is a leading provider of Behavioral Attack Detection solutions that provide accurate and efficient security visibility into attacks that have slipped through the cracks of traditional security controls. The LightCyber Magna™ platform is the first security product to integrate user, network and endpoint context to provide security visibility into a range of attack activity. Founded in 2012 and led by world-class cyber security experts, the company's products have been successfully deployed by top-tier customers around the world in industries including the financial, legal, telecom, government, media and technology sectors. For more information, please visit http://www.lightcyber.com

LIGHTCYBER
5050 El Camino, Suite 226
Los Altos, CA
Ph: (844) 560-7976
www.lightcyber.com